El código 2.0

Lawrence Lessig

VERSIÓN 2.0

traficantes de sueños

mapas



Desde sus inicios **Traficantes de Sueños** ha apostado por licencias de publicación que permiten compartir, como las Creative Commons, por eso sus libros se pueden copiar, distribuir, comunicar públicamente y descargar desde su web. Entendemos que el conocimiento y las expresiones artísticas se producen a partir de elementos previos y contemporáneos, gracias a las redes difusas en las que participamos. Están hechas de retazos, de mezclas, de experiencias colectivas; cada persona las recompone de una forma original, pero no se puede atribuir su propiedad total y excluir a otros de su uso o replicación.

Sin embargo, «cultura libre» no es sinónimo de «cultura gratis». Producir un libro conlleva costes de derechos de autor, traducción, edición, corrección, maquetación, diseño e impresión. Tú puedes colaborar haciendo una donación al proyecto editorial; con ello estarás contribuyendo a la liberación de contenidos.

Puedes hacer una donación
(si estás fuera de España a través de PayPal),
suscribirte a la editorial
o escribirnos un mail

El código 2.0

Lawrence Lessig

traficantes de sueños

Traficantes de Sueños no es una casa editorial, ni siquiera una editorial independiente que contempla la publicación de una colección variable de textos críticos. Es, por el contrario, un proyecto, en el sentido estricto de «apuesta», que se dirige a cartografiar las líneas constituyentes de otras formas de vida. La construcción teórica y práctica de la caja de herramientas que, con palabras propias, puede componer el ciclo de luchas de las próximas décadas.

Sin complacencias con la arcaica sacralidad del libro, sin concesiones con el narcisismo literario, sin lealtad alguna a los usurpadores del saber, TdS adopta sin ambages la libertad de acceso al conocimiento. Queda, por tanto, permitida y abierta la reproducción total o parcial de los textos publicados, en cualquier formato imaginable, salvo por explícita voluntad del autor o de la autora y sólo en el caso de las ediciones con ánimo de lucro.

Omnia sunt communia!

mapas 24

Mapas. Cartas para orientarse en la geografía variable de la nueva composición del trabajo, de la movilidad entre fronteras, de las transformaciones urbanas. Mutaciones veloces que exigen la introducción de líneas de fuerza a través de las discusiones de mayor potencia en el horizonte global.

Mapas recoge y traduce algunos ensayos, que con lucidez y una gran fuerza expresiva han sabido reconocer las posibilidades políticas contenidas en el relieve sinuoso y controvertido de los nuevos planos de la existencia.

Edición original: *The Code version 2.0*, Cambridge, Basic Books, 2006.

1ª edición: 1000 ejemplares
Mayo de 2009
Título:
El código 2.0
Autor:
Lawrence Lessig
Edición e introducción:
Florencio Cabello
Traducción:
María Acuyo, María del Mar Alonso, Manuel Astorga, Sandra Burgos, Nicolás Castán, Raquel Castro, Clara Chicón, Francisca Castro, Virginia del Río, Ana Delgado, Carmen Dugo, Giulia Faraguna, Carola Felis, Carolina Flores, Macarena Florido, Beatriz Galdón, Natalia Gnisci, Leticia González, Olga Gutiérrez, Vanessa Gutiérrez, Sophia Lara-Matheu, Paloma Mancheño, Beatriz Martínez, Marta Morales, María de la Paz Moreno, Marina Navas, Patricia Navas, Luis Miguel Núñez, Juan Manuel Ortega, Pilar Palomino, Adrián Pardo, Ana Pérez Pedrosa, Ángel María Pulido, Beatriz Rando, Ana Sánchez, Néstor Sánchez, Vanessa Sánchez, Nadia Sanhaji, Michael Schmidt, María Sorzano, Ana María Torrado, Laura Vacas y Carmen Vargas
Maquetación y diseño de cubierta:
Taller de diseño Traficantes de Sueños.
Edición:
Traficantes de Sueños
C/Embajadores 35
28012 Madrid. Tlf: 915320928
e-mail:editorial@traficantes.net
http://traficantes.net
Impresión:
Queimada Gráficas.
C/ Salitre, 15 28012, Madrid
Tlf: 915305211
ISBN: 978-84-96453-38-8
Depósito legal: M-19814-2009

El código 2.0

Lawrence Lessig

Edición e introducción
Florencio Cabello

Traducción
María Acuyo, María del Mar Alonso, Manuel Astorga, Sandra Burgos, Nicolás Castán, Raquel Castro, Clara Chicón, Francisca Castro, Virginia del Río, Ana Delgado, Carmen Dugo, Giulia Faraguna, Carola Felis, Carolina Flores, Macarena Florido, Beatriz Galdón, Natalia Gnisci, Leticia González, Olga Gutiérrez, Vanessa Gutiérrez, Sophia Lara-Matheu, Paloma Mancheño, Beatriz Martínez, Marta Morales, María de la Paz Moreno, Marina Navas, Patricia Navas, Luis Miguel Núñez, Juan Manuel Ortega, Pilar Palomino, Adrián Pardo, Ana Pérez Pedrosa, Ángel María Pulido, Beatriz Rando, Ana Sánchez, Néstor Sánchez, Vanessa Sánchez, Nadia Sanhaji, Michael Schmidt, María Sorzano, Ana María Torrado, Laura Vacas y Carmen Vargas

traficantes de sueños
mapas

Índice

Introducción

Florencio Cabello

Descuide quien lea estas líneas que ellas no están destinadas a remedar por anticipado las ideas de esta obra, para demostrar lo avispado que soy o lo atinada que ha sido la iniciativa de editarla en castellano. Nada más lejos de mi intención. Y ello no sólo (y eso sería ya suficiente motivo) porque a continuación vienen nada menos que dos prefacios que presentan detalladamente los aspectos cruciales de las dos versiones de esta *obra abierta*, sino porque a estas alturas ni *El código* ni su autor requieren apenas presentación.

Por lo que respecta a la obra, quienes leyeran su primera versión coincidirán en que hace tiempo que alcanzó la categoría de clásico moderno sobre la tecnología y el ciberespacio, aunque sólo sea por la cantidad de veces que *no* se la cita al utilizar sus argumentos (prueba inequívoca de la condición adquirida). En este sentido, *El código 2.0* brinda la oportunidad de (re)conocer el complejo y ambivalente territorio de las redes de comunicación digitales a través de una cartografía que mantiene intacto el carácter seminal del libro original (que supuso, sin ir más lejos, el preludio de la fundación de Creative Commons) al tiempo que *abre su código fuente* (ver «Prefacio» a la Segunda Edición) para contrastar sus coordenadas con los más recientes desplazamientos producidos en dicho territorio. En efecto, esta obra (al igual que su autor) atraviesa de forma envidiablemente brillante las fronteras disciplinares que pretenden privarnos de una aprehensión profunda de las matrices históricas, las mediaciones sociales y los conflictos políticos y culturales que hoy se nos presentan *cifrados* bajo las consabidas etiquetas de la «sociedad del conocimiento» o «sociedad de la información».

Felizmente Lessig demuestra aquí sus formidables dotes para la criptografía y descifra con sencillez y precisión la maraña de argucias, sofismas y malentendidos que camuflan bajo capa de «naturaleza», «necesidad» o incluso de «equilibrio» lo que no son sino decisiones que responden a unos principios determinados (y ello para bien y para mal). Si no contáramos con la suerte de conocer a abogados como Javier de la Cueva o David Bravo, podríamos afirmar que Lessig constituye una *rara avis* dentro del campo jurídico, por su afán por (y su éxito en) desentrañar los desafíos democráticos que atraviesan la constitución actual del ciberespacio.

Lo cierto es, no obstante, que la singularidad de Lessig no acaba ni mucho menos en lo que concierne a la abogacía. ¿O acaso es habitual que un catedrático de la Universidad de Stanford cuelgue su obra en un *wiki* para que cualquier estudiante o curioso pueda enmendarle la plana? ¿Abundan los autores célebres que sean coherentes con los discursos trufados de libertad y publiquen sus obras bajo una licencia libre que permite su copia y modificación con cualquier propósito? En fin, y aquí me incluyo como docente novato, ¿cuántos profesores universitarios no hacemos honor a aquella máxima de George Bernard Shaw según la cual *He who can, does. He who cannot, teaches* («El que puede, lo hace. El que no, enseña»)?

Sea como fuere, el propósito de esta presentación es contar algo que la mayoría de lectores no sepa (a diferencia de lo anterior), algo que resulta complicado captar al manejar el formato físico del libro, o incluso el formato electrónico en que haya sido descargado. Ya mencioné previamente que las claves originales del proceso al que aludo las detalla Lessig en el Prefacio a la Segunda Edición, pero creo que merece la pena explicar brevemente la parte correspondiente a la traducción y edición en castellano.

En este sentido, considero pertinente abrir dicha explicación con un apunte que remite a la crítica de la economía política clásica que el sociólogo Maurizio Lazzarato rastrea en la obra de su homólogo francés Gabriel Tarde. En efecto, para dar cuenta del proceso de elaboración de la obra que el lector tiene en sus manos (o en la pantalla de su ordenador, móvil, etc.), parto del mismo interrogante con que Tarde invierte en 1902 el punto de partida del análisis económico canónico y su modelo de la fábrica de alfileres de Adam Smith: «¿Cómo se hace un libro? ¿No resulta menos interesante que saber cómo se elabora un alfiler o un botón?».[1]

---

[1] Gabriel Tarde, *Psychologie économique*, París, Felix Alcan, 1902, p. 91, citado en Maurizio Lazzarato, «Tradición cultural europea y nuevas formas de producción y transmisión del saber», en *Capitalismo cognitivo*, Traficantes de Sueños, Madrid, 2004, p. 131.

Antes de nada hay que insistir en la decisiva importancia de la apuesta de Lawrence Lessig por dar pie a un proceso cooperativo y descentralizado de revisión de su obra original y, más allá, de acceso a ella para realizar obras derivadas. Tal apuesta es la que inspira la creación de un proyecto de traducción al castellano de su obra, así como la metodología de trabajo adoptada para dicha labor. Sin este modelo (acompañado del apoyo y seguimiento entusiastas que Lessig mantiene desde que conoce el proyecto), la tarea planteada habría resultado extremadamente difícil de acometer.

Así pues, la presente edición en castellano de *El código 2.0* es fruto del trabajo de un grupo de investigación/traducción compuesto por 43 estudiantes de la Universidad de Málaga (UMA) y por mí como coordinador. Los nombres de estos estudiantes aparecen al principio del libro, pero deseo repetirlos aquí en un tipo de letra mayor: María Acuyo, María del Mar Alonso, Manuel Astorga, Sandra Burgos, Nicolás Castán, Raquel Castro, Clara Chicón, Francisca Castro, Virginia del Río, Ana Delgado, Carmen Dugo, Giulia Faraguna, Carola Felis, Carolina Flores, Macarena Florido, Beatriz Galdón, Natalia Gnisci, Leticia González, Olga Gutiérrez, Vanessa Gutiérrez, Sophia Lara-Matheu, Paloma Mancheño, Beatriz Martínez, Marta Morales, María de la Paz Moreno, Marina Navas, Patricia Navas, Luis Miguel Núñez, Juan Manuel Ortega, Pilar Palomino, Adrián Pardo, Ana Pérez Pedrosa, Ángel María Pulido, Beatriz Rando, Ana Sánchez, Néstor Sánchez, Vanessa Sánchez, Nadia Sanhaji, Michael Schmidt, María Sorzano, Ana María Torrado, Laura Vacas y Carmen Vargas.

Dicho grupo nace de una propuesta paralela de trabajo que planteé a los estudiantes de 2º de Publicidad y Relaciones Públicas de la Facultad de Ciencias de la Comunicación de Málaga en el marco de la asignatura Tecnología de la Comunicación Audiovisual. Mi intención era enfocar dicha asignatura hacia la tecnología digital y el ciberespacio mediante el estudio de *El código* de Lessig, pero era obvio que debíamos recurrir a la reciente actualización de la obra y no a la traducción castellana de la primera versión editada por Taurus en 2001. La cuestión era que necesitábamos urgentemente una traducción de *Code 2.0* sobre la que trabajar, y sería absurdo que un docente no contara con el potencial de sus estudiantes para conseguir ese propósito que nos beneficiaría a todos.

De este modo, el primer día de clase (25 de febrero de 2008) lancé a los propios estudiantes mi propuesta explicando su doble objetivo pedagógico e investigador. Por una parte, se trataba de que asumieran un mayor protagonismo en su proceso de aprendizaje, convirtiéndose en coautores de su propio material didáctico y, más allá, en suministradores de un *legado* que recibirían y completarían a su vez las siguientes promociones que cursaran la asignatura.

Por otro lado, se trataba de poner en marcha un experimento de producción de conocimiento por parte de estudiantes cuyo trabajo de clase no quedaría ya arrumbado en el cajón de un despacho, sino que adquiriría una repercusión amplia mediante su publicación electrónica y en papel. Aquí la plena confianza depositada en nosotros por Traficantes de Sueños también resultó decisiva para emprender el proyecto.

A partir de esta propuesta se conformó un grupo de una treintena de estudiantes (a los que se fueron uniendo luego otros, incluso procedentes de titulaciones distintas) entre los que distribuimos los distintos capítulos de la obra. El siguiente paso fue abrir un *wiki* en el que poder volcar de forma cooperativa y descentralizada nuestros periódicos avances en la traducción, revisar y corregir los de los demás y elaborar un glosario de términos recurrentes con el que garantizar la homogeneidad de una escritura a 44 manos. En este sentido, quiero expresar mi agradecimiento al Servicio de Enseñanza Virtual de la UMA por proporcionarnos la estupenda herramienta del Campus Virtual, y especialmente a Beatriz Rando por introducirme a su manejo. En último término, la labor virtual en dicho *wiki* se complementó con reuniones presenciales con los distintos «capitanes –responsables– de capítulo», en las que comentábamos el trabajo realizado y discutíamos la versión final de cada una de las secciones antes de *liberarla* para que la leyera el resto de estudiantes.

A finales del cuatrimestre dispusimos ya de una primera versión casi completa de la traducción, la cual pasé a revisar para darle su forma definitiva, añadir notas aclaratorias y corregir erratas. A este último respecto quiero destacar también la labor de muchos estudiantes que, sin colaborar en el grupo de traducción, nos fueron señalando minuciosamente las erratas que encontraban a medida que iban leyendo nuestro texto en clase. A modo de provocación, cabría afirmar que bendita la masificación universitaria que permite cooperar a un grupo de 43 estudiantes/investigadores/traductores y contar con otra veintena de lectores/correctores.

Por último, deseo agradecer especialmente el apoyo que ha brindado al proyecto Javier de la Cueva, así como su inagotable paciencia para atender mis múltiples consultas telefónicas sobre terminología jurídica. Por más que buena parte de las referencias políticas y legales puedan extrapolarse sin grandes dificultades del contexto estadounidense al europeo y español (y ello, una vez más, para bien y para mal), la contribución de Javier de la Cueva ha permitido precisar la traducción de numerosos términos jurídicos respetando los matices existentes en la legislación de copyright estadounidense y en la española de derecho de autor. En este sentido, los errores que aún puedan quedar son exclusivamente atribuibles al editor.

Sólo me resta, antes de cerrar esta presentación, invitar a todos los lectores interesados en conocer más sobre el proceso de traducción, o en consultar nuestro glosario de términos técnicos, a que visiten nuestro *wiki* (pulsando en «Entrar como invitado») en la dirección:
http://cccom.cv.uma.es/mod/resource/view.php?id=10955vvv.

Prefacio a la primera edición

En la primavera de 1996 y en el marco de un congreso anual titulado «Ordenadores, libertad y privacidad», se invitó a dos escritores de ciencia ficción a fabular acerca del futuro del ciberespacio. El primero de ellos, Vernor Vinge, habló de una «aplicación ubicua de la ley» posibilitada por «sistemas distribuidos de grano fino» en los que la tecnología que facilita nuestro modo futuro de vida también suministra información al Estado y se somete a sus órdenes. Tal arquitectura se encontraba ya en construcción —no era otra que Internet— y los tecnólogos estaban ya describiendo cómo extenderla. A medida que la red que permitía tal control se iba entretejiendo con cada una de las partes de la vida social, sería cuestión de tiempo, aseguraba Vinge, que el Estado reclamara controlar partes vitales de dicho sistema. A medida que el sistema madurase, cada nueva generación de código no haría sino incrementar el poder del Estado. Nuestros *yoes digitales* —también cada vez más los físicos— vivirían en un mundo de regulación perfecta propiciada por la arquitectura de computación distribuida —Internet y sus sucesoras.

A continuación Tom Maddox contó una historia similar a la de Vinge, pero con una distribución de papeles ligeramente diferente. El poder estatal no provendría exclusivamente de los chips, argüía Maddox, sino que se reforzaría mediante una alianza entre el Estado y el comercio. Al comercio, como al Estado, le conviene un mundo cada vez más regulado. Por consiguiente, el comercio estaría dispuesto a contribuir, directa o indirectamente, a su construcción. De este modo, el ciberespacio se transformaría hasta adquirir características propicias a estas dos poderosas fuerzas de orden social. Y en la otrora volátil y salvaje Internet habría que dar cuentas por todo.

Código y comercio.

Cuando Vinge y Maddox hablaron, el futuro que describían aún no estaba presente. El ciberespacio se expandía ya por doquier, pero a su auditorio le resultaba muy complicado imaginárselo sometido a los fines del Estado. Y ciertamente el comercio en aquel momento se interesaba por el ciberespacio, pero las empresas de tarjetas de crédito seguían advirtiendo a sus clientes de que se mantuvieran bien alejados de la red. Se veía que la red era un incipiente espacio social, pero costaba vislumbrarla como un incipiente espacio *de control social*.

Yo no escuché a Vinge y Maddox aquel día, sino tres años después, a través de mi computadora. Sus palabras habían sido grabadas y ahora están archivadas en un servidor del MIT (*Massachusetts Institute of Technology*, Instituto Tecnológico de Massachusetts).[1] Basta un segundo para acceder al archivo con sus intervenciones. El acto mismo de escuchar estas conferencias pronunciadas hace años —a través de una plataforma perfectamente fiable e indexada que, sin duda alguna, registró mi acceso mediante la conexión de alta velocidad que lleva a mi casa Internet y el canal ABC News— suponía una confirmación parcial de su relato. A juzgar por la reacción del auditorio registrada en la grabación, éste asumía que lo que escuchaba era pura fábula —después de todo, los ponentes eran escritores de ciencia ficción—, y que estaban aterrorizados ante esas ideas.

Diez años después, los relatos de Vinge y Maddox ya no son ciencia ficción. Ya no resulta complicado entender cómo la red podría devenir un espacio perfectamente regulado o cómo podrían contribuir a ello los intereses comerciales.

La batalla actual en torno a compartir archivos en redes de pares (P2P) constituye un ejemplo paradigmático al respecto. A la vista del ingente volumen de archivos de música (entre otros) intercambiados de forma gratuita (e ilegal)[2]

---

1 VI Congreso «Ordenadores, libertad y privacidad». Véase http://mit.edu/cfp96/www/.

2 El autor alude siempre a la legislación estadounidense. En España la situación es distinta, pues la legalidad de compartir archivos sin ánimo de lucro aún es objeto de controversia, centrada básicamente en si cabe o no ampararla en el derecho de copia privada consagrado en el Artículo 31.2 de la Ley 23/2006, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual. Así, en la Circular 1/2006, 5 de mayo de 2006, sobre los delitos contra la propiedad intelectual e industrial el Fiscal General del Estado expone que el intercambio P2P, «...sin perjuicio de poder constituir un ilícito civil», no es un delito si no entraña «un ánimo de lucro comercial» (p. 37), alegando que no es «posible, ni efectiva, una criminalización de la sociedad» (p. 99). Tal doctrina ha sido respaldada por el Parlamento Europeo, que el 25 de abril de 2007 aprobó la propuesta modificada de Directiva *relativa a las medidas penales destinadas a garantizar el respeto de los derechos de propiedad intelectual (2005/0127(COD)), donde incluyó una enmienda al artículo 2 que excluye la punibilidad de «los actos efectuados por usuarios privados con fines personales y no lucrativos».* [N. del E.]

mediante programas P2P, la industria discográfica ha contraatacado. Su estrategia ha incluido feroces demandas contra quienes descargan música ilegalmente, esfuerzos extraordinarios para promover nuevas leyes que refuercen la protección del copyright y una batería de medidas tecnológicas concebidas para alterar un rasgo de la arquitectura original de redes —a saber, que Internet reproduce contenidos sin atender a si están o no sujetos a copyright. La batalla ya ha comenzado y de su resultado dependerá mucho más que la mera distribución musical. Lo que sí está claro es el campo de batalla: el comercio y el Estado colaborando para conseguir una infraestructura que permita un mayor control.

Vinge y Maddox pertenecían a la primera generación de teóricos del ciberespacio. Podían fabular acerca del control perfecto porque vivían en un mundo que no podía ser controlado. Podían conectar con el público porque éste deseaba resistirse al futuro que ellos describían. De hecho, imaginar ese mundo imposible llegó a ser un *deporte nacional*.

Ahora lo imposible se está haciendo realidad. Buena parte del control descrito por Vinge y Maddox ante la estupefacción de un auditorio que lo consideraba orwelliano resulta ahora muy razonable para muchos. No sólo es posible imaginar el sistema de regulación perfecta descrito por Vinge, sino que a algunos les agrada. Resulta inevitable que el comercio acapare parcelas cada vez más vastas de Internet y la mayoría de la gente tampoco ve nada malo en ello. Hoy día lo «terrorífico» se ha vuelto normal y sólo los historiadores (y los autores de viejos libros como éste) percibirán la diferencia.

Esta obra retoma los relatos de Vinge y Maddox, cuya visión del futuro de la red comparto; en buena parte nos ocuparemos de la arquitectura de regulación expansiva en que se convertirá Internet. Lo que no comparto es la satisfacción de los vítores autocomplacientes que resuenan de fondo en la grabación de 1996. Puede que fuera obvio quién era «el enemigo» en 1996; hoy no lo es.

La tesis de este libro es que nuestro futuro no coincide con los relatos de Vinge y Maddox entendidos por separado, sino que es una combinación de ambos. Si sólo aceptáramos la distopía de Vinge, dispondríamos de una respuesta obvia y poderosa: Orwell nos dio las herramientas y Stalin la determinación para resistirnos a un Estado totalitario. Tras el 11-S, hemos de vérnoslas con una red espía e invasiva, pero que tiene sus límites. Nuestro futuro no es el control totalitario desde Washington; *1984* pertenece definitivamente a nuestro pasado.

Del mismo modo, si sólo aceptáramos el futuro que describió Maddox, muchos de nuestros conciudadanos no lo considerarían ciencia ficción, sino toda una utopía. Para ellos, un mundo donde «el mercado» campara a sus anchas y el «mal» estatal fuera derrotado sería un mundo de libertad perfecta.

Ahora bien, cuando combinamos los futuros que describieron Vinge y Maddox, nos encontramos ante una imagen completamente diferente: un futuro de control ejercido en gran medida mediante las tecnologías del comercio, respaldadas por el imperio de la ley (o lo que queda de él).

El desafío de nuestra generación es reconciliar estas dos fuerzas. ¿Cómo protegemos la libertad cuando las arquitecturas de control están gestionadas tanto por el Estado como por el sector privado? ¿Cómo aseguramos la privacidad cuando el *éter* nos espía a perpetuidad? ¿Cómo garantizamos el pensamiento libre cuando se reclama la propiedad privada de las ideas? ¿Cómo garantizamos la autodeterminación cuando las arquitecturas de control siempre las determinan otros? En otras palabras, ¿cómo construimos un mundo de libertad afrontando los peligros que Vinge y Maddox describieron conjuntamente?

La respuesta no se halla en la visceral retórica antiestatal de un pasado liberal: los Estados son necesarios para proteger la libertad, pese a que también sean muy capaces de destruirla. Pero la respuesta tampoco reside en un retorno al *New Deal* de Roosevelt. El estatismo ha fracasado. La libertad no se encuentra en ninguna sopa de letras burocrática de Washington (WPA, FCC, FDA…).

Una segunda generación de teóricos del ciberespacio ha rescatado los ideales de la primera y los está desarrollando en circunstancias diferentes. Conocen bien los debates del pasado y han cartografiado los «argumentos-callejones sin salida» de los últimos treinta años. Su objetivo es plantear interrogantes que sorteen dichos callejones sin salida y los superen.

Ambas generaciones son muy prolíficas. Esther Dyson, John Perry Barlow y Todd Lapin todavía resultan inspiradores y siguen en la brecha (Dyson es editora general de CNET Networks; Barlow colabora actualmente en Harvard). En cuanto a la segunda generación, las obras de Andrew Shapiro, David Shenk y Steven Johnson están cosechando gran difusión y admiración.

Mi objetivo es esta segunda generación. Como corresponde a mi profesión (soy abogado), mi contribución es más prolija, más oscura, más técnica y más obtusa que las mejores de cualquiera de las dos generaciones.

Pero como corresponde a mi profesión, la expondré de todas formas. En medio de los acalorados debates actuales, lo que tengo que decir no complacerá a nadie. Mientras tecleo estas últimas palabras antes de enviar el manuscrito a mi editor, me parece estar escuchando ya las reacciones: «¿Es que acaso no ves la diferencia entre el poder del *sheriff* y el de Walt Disney?», «¿de verdad crees que necesitamos una agencia estatal que regule el código informático?». Y del otro lado: «¿Cómo se te ocurre defender una arquitectura del ciberespacio (el software libre) que inhibe la capacidad del Estado para hacer el bien?».

No obstante, soy profesor además de abogado. Si mis textos provocan reacciones airadas, acaso también puedan incitar reflexiones más equilibradas. Vivimos tiempos en que no resulta nada fácil atinar, pero las respuestas fáciles a los debates del pasado no son las adecuadas en el presente.

He aprendido mucho de los profesores y críticos que me han ayudado a escribir este libro. Hal Abelson, Bruce Ackerman, James Boyle, Jack Goldsmith y Richard Posner me proporcionaron magníficos y pacientes consejos con respecto a los primeros borradores. Les agradezco su paciencia y me siento muy afortunado de haber contado con sus consejos. Larry Vale y Sarah Whiting orientaron mis lecturas en el campo de la arquitectura, aunque no cabe duda de que debería haber sido un estudiante más paciente de lo que fui. Sonya Mead me ayudó a poner en imágenes lo que a un abogado le habría costado decir mucho más de mil palabras.

Un ejército de estudiantes libró la mayor parte de la batalla con los primeros borradores de este libro. Carolyn Bane, Rachel Barber, Enoch Chang, Ben Edelman, Timothy Ehrlich, Dawn Farber, Melanie Glickson, Bethany Glover, Nerlyn Gonzalez, Shannon Johnson, Karen King, Alex Macgillivray, Marcus Maher, David Melaugh, Teresa Ou, Laura Pirri y Wendy Seltzer me ofrecieron sus críticas amplias y siempre respetuosas. Y mis ayudantes, Lee Hopkins y Catherine Cho, resultaron cruciales para mantener este ejército en formación (y a raya).

Tres colegas en especial han influido en mi tesis. Harold Reeves tomó las riendas del Capítulo 10, Tim Wu me obligó a repensar en buena medida la primera parte y Andrew Shapiro me mostró su esperanza en un futuro que he descrito de forma bastante sombría.

Me siento especialmente en deuda con Catherine Marguerite Manley, cuyo extraordinario talento como escritora y como investigadora me permitió acabar esta obra mucho antes de lo que lo habría hecho. Mi agradecimiento también a Tawen Chang y James Stahir por su cuidadosa revisión de las notas y su esfuerzo para mantener su exactitud.

Éste no es un campo que se pueda investigar encerrado en la biblioteca. Todo lo que sé lo he aprendido gracias a conversaciones que he mantenido, o presenciado, con una extraordinaria comunidad de académicos y activistas que llevan años luchando para comprender qué es el ciberespacio y para mejorarlo. Esta comunidad incluye a los eruditos y escritores que aparecen en el texto, especialmente a los abogados Yochai Benkler, James Boyle, Mark Lemley, David Post y Pam Samuelson. Asimismo, he obtenido un gran provecho de conversaciones con personas no vinculadas a la abogacía, especialmente con Hal Abelson, John Perry Barlow, Todd Lapin, Joseph Reagle, Paul Resnick y Danny Weitzner. Pero quizá lo más importante hayan sido las discusiones con los activistas, especialmente con los del *Center for Democracy and Technology*, de la *Electronic Frontier Foundation* y del *American Civil Liberties Union*. Ellos han llevado los debates a la realidad y han hecho mucho por defender al menos algunos de los principios que estimo importantes.

Sea como fuere, nunca habría escrito este libro si no fuera por un relato de Julian Dibbell, por un congreso organizado por Henry J. Perritt y por las muchas discusiones que he mantenido con David Johnson. A los tres les estoy muy agradecido por todo lo que me han enseñado.

Comencé este proyecto como investigador del Programa de Ética y Profesiones de la Universidad de Harvard, y agradezco a Dennis Thompson el apoyo escéptico que me ofreció aquel año. El *Berkman Center for Internet and Society* de la Facultad de Derecho de Harvard me ha permitido desarrollar buena parte de mi investigación. Estoy muy agradecido a Lillian y Myles Berkman por ese apoyo, y de forma especial al codirector del centro y colega ocasional, Jonathan Zittrain, por brindarme su ánimo y, lo que es más importante, su amistad. He querido dedicar este libro al otro codirector del *Berkman Center*, Charlie Nesson, que me ha proporcionado espacio y apoyo para realizar esta obra, además de cierta inspiración para abordarla de forma diferente.

No obstante, por encima de todo este apoyo está la paciencia y el amor de la persona a la que he consagrado mi vida, Bettina Neuefeind. Su amor seguirá pareciendo descabellado y maravilloso durante mucho más de un año.

Prefacio a la segunda edición

Ésta es una transformación de un viejo libro —es más, en tiempos de Internet, una transformación de un texto arcaico. La primera edición se publicó en 1999. El libro fue escrito en un contexto muy diferente y, en buena parte, en oposición a ese contexto. Tal y como describo en el primer capítulo, entre aquéllos que por entonces parloteaban sobre el ciberespacio, la idea dominante era que éste se hallaba fuera del alcance de la regulación del espacio real. El Estado no podía tocar la vida *online*. De ahí se desprendía que esta vida sería distinta e independiente de la dinámica de la vida *offline*. La primera versión de *El código* venía a refutar lo que en aquel momento era una creencia común.

Tal creencia común se ha esfumado con el paso de los años. La confianza de los excepcionalistas de Internet se ha debilitado. La idea —e incluso el deseo— de que Internet quedara al margen de regulaciones ha desaparecido. He aquí que, cuando acepté la invitación a reeditar esta obra, me enfrenté a un difícil dilema: o bien escribir un libro nuevo, o bien actualizar el anterior para que mantuviera su relevancia e interés en un momento radicalmente diferente.

He optado por esto último. La estructura básica de la primera edición permanece intacta y la tesis es la misma. Sí que he revisado el enfoque de ciertos ejemplos concretos y, así lo espero, la claridad de la redacción. También he ampliado la tesis en algunas partes y para integrarla mejor, he añadido breves enlaces a trabajos posteriores.

Algo que no he hecho, sin embargo, es desarrollar la tesis de este libro allá donde otros han trabajado. Tampoco he sucumbido a la tentación (insensatamente poderosa) de rescribir el libro a modo de contestación a los

críticos, indulgentes o no. En las notas he incluido indicaciones para quien desee indagar los argumentos que otros han contrapuesto a los míos. Ahora bien, este libro constituye, hoy más aún que en 1999, sólo una pequeña parte de un debate mucho mayor. Así pues, no debería leerse sin considerar otras extraordinarias obras posteriores. En particular hay dos libros recientes que complementan muy bien la tesis que aquí defiendo: *Who Controls the Net?* (2006), de Goldsmith y Wu y *The Wealth of Networks* (2006) de Benkler —más un tercero, escrito por Zittrain y esperado para 2007, que la desarrolla significativamente.[1]

No he tratado tampoco de enumerar los errores, reales o supuestos, cometidos en la primera edición. Algunos los he corregido simplemente y otros los he dejado, porque, por más equivocados que les parezcan a algunos, yo sigo creyendo que no son errores. Entre ellos el más destacado es mi percepción de que la infraestructura de Internet será cada vez más controlada y regulable a través de tecnologías de identificación digital. Algunos amigos han calificado este «error» de «mentira». No lo es. No estoy seguro de qué horizonte temporal tenía en mente en 1999, y admito que ciertas predicciones formuladas entonces no se han cumplido —todavía. Pero estoy más convencido de ello hoy que entonces, por lo que he decidido aferrarme a este «error fundamental». Quizá se trate tan sólo de cubrirme las espaldas: si estoy en lo cierto, obtendré la recompensa de la comprensión; si me equivoco, tendremos una red más cercana a los principios de su diseño original.

La génesis de la presente revisión se basó en un *wiki*. Basic Books me permitió colgar la edición original del libro en un *wiki* alojado por Jotspot y un equipo de «capitanes –responsables de capítulo» ayudó a incitar un coloquio acerca del texto. Hubo algunas modificaciones al texto mismo, así como numerosos comentarios y críticas de gran valor.[2] A continuación tomé el texto resultante a finales de 2005 y le agregué mis propias aportaciones para producir este libro. Aunque yo no iría tan lejos como el músico Jeff Tweedy (*Half of it's you, half is me* —«Una mitad es vuestra, la otra es mía»), una parte importante de esta obra no es mía. En reconocimiento a ello, he destinado los ingresos por derechos de autor de este libro a la organización sin ánimo de lucro *Creative Commons*.

---

1 El autor alude al libro de Jonathan Zittrain, *The Future of the Internet—And How to Stop It*, publicado en 2008 por Yale University Press y Penguin UK. Las referencias de los otros dos libros son: Jack Goldsmith y Tim Wu, *Who controls the Net? Illusions of a Borderless World*, Nueva York, Oxford University Press, 2006 y Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven, Yale University Press, 2006. [N. del E.]

2 El *wiki* sigue vivo en http://codev2.cc y todos los enlaces de hipertexto citados se encuentran disponibles en http://codev2.cc/links.

Agradezco a JotSpot (<jot.com>) que donara el *wiki* y el alojamiento usados para editar la primera versión de *El código*. Dicho *wiki* fue administrado por un extraordinario estudiante de Stanford, Jake Wachman, que destinó a este proyecto más tiempo del que tenía. Cada capítulo del libro, mientras vivía en el *wiki*, tenía un «capitán de capítulo». A todos ellos —Ann Bartow, Richard Belew, Seth Finkelstein, Joel Flynn, Mia Garlick, Matt Goodell, Paul Gowder, Peter Harter, Brian Honermann, Brad Johnson, Jay Kesan, John Logie, Tom Maddox, Ellen Rigsby y Jon Stewart— les estoy agradecido por el trabajo que se ofrecieron a realizar, así como a los muchos voluntarios que dedicaron su tiempo a intentar mejorar la primera versión de *El Código*. Estoy especialmente agradecido a Andy Oram por sus extensas contribuciones al *wiki*.

Junto a estos voluntarios, Stanford me ayudó a reunir un ejército de estudiantes de Derecho que contribuyó a completar la investigación que *El código 2.0* requería. Comenzaron cuatro de ellos —David Ryan Brumberg, Jyh-An Lee, Bret Logue y Adam Pugh—, dedicando un verano a recopilar todas las obras que se basaban en *El código* o lo criticaban. Sobre esa base decidí en parte cómo modificar la obra. Durante el segundo semestre de 2005, un seminario de estudiantes de Stanford aportó su propio enfoque crítico, como también hicieron desde la Facultad de Derecho de Cardozo. Y durante ese año otros dos estudiantes, John Eden y Avi Lev Robin-Mosher, pasaron muchas horas ayudándome a ultimar la investigación necesaria para completar un borrador razonable de *El código 2.0*.

No obstante, ningún estudiante contribuyó tanto a la versión final de este libro como Christina Gagnier. En los últimos meses del proyecto ella tomó las riendas de la investigación, completando un cúmulo de cuestiones sin resolver, dando a los resultados de este proceso de año y medio una forma que se pudiera publicar y supervisando un repaso de todas las citas para verificar su integridad y exactitud. Sin su trabajo, nunca se habría completado este libro.

Asimismo, estoy agradecido a los amigos y colegas que me han ayudado a ver posibles transformaciones de este trabajo —especialmente a Ed Felten, David Johnson, Jorge Lima, Alan Rothman y Tim Wu. Jason Ralls elaboró el diseño gráfico de *El código 2.0*. Y finalmente, no tengo palabras para expresar cuánto debo a Elaine Adolfo, cuyo talento y paciencia sobrepasan cuanto haya podido conocer jamás, y sin la cual poco podría haber hecho en los últimos años, incluido esto.

1. El código es la ley

HACE CASI DOS DÉCADAS, en la primavera de 1989, el comunismo murió en Europa —se derrumbó, como una tienda de campaña a la que quitaran el poste central. Su final no llegó por medio de guerras o revoluciones; llegó por puro agotamiento. En Europa Central y Oriental el comunismo dio paso al nacimiento de un nuevo régimen, al comienzo de una nueva sociedad política.

Para los estudiosos del Derecho Constitucional (como yo), ésa fue una época fascinante. Yo había acabado Derecho en 1989 y en 1991 comencé a dar clases en la Universidad de Chicago. Allí existía por entonces un centro dedicado al estudio de las democracias emergentes en Europa Central y Oriental, del cual pasé a formar parte. Durante los cinco años siguientes pasé más horas en aviones y aeropuertos y más mañanas desayunando un café pésimo de las que quiero recordar.

Europa Central y Oriental se llenó de estadounidenses que explicaban a los ex-comunistas cómo debían gobernarse, ofreciéndoles un sinfín de consejos, a cada cual más ridículo. Alguno de estos visitantes se dedicaba, literalmente, a vender constituciones a las emergentes repúblicas constitucionales; el resto rebosaba de ideas atolondradas sobre el modo en que debía gobernarse una nación. Estos estadounidenses procedían de una nación donde el constitucionalismo parecía funcionar, pero ni ellos sabían por qué.

La misión de mi centro, en cambio, no consistía en ofrecer consejos. Nos quedaba mucho por aprender como para guiar a nadie. Nuestro propósito era observar y recopilar información acerca de las transiciones y de cómo iban progresando. Pretendíamos entender el cambio, no dirigirlo.

Lo que allí observamos fue sorprendente, aunque comprensible. Aquellos primeros momentos posteriores al colapso del comunismo rebosaban de pasión antiestatal —una oleada de furia contra el Estado y contra toda regulación proveniente del mismo. «Déjennos en paz», parecía decir la gente. «Dejen que el mercado y las organizaciones no gubernamentales —una nueva sociedad— reemplacen al Estado». Tras varias generaciones de comunismo, esta reacción resultaba más que comprensible. El Estado era el opresor, así que ¿qué compromiso se podía esperar que tuvieran con respecto al instrumento mismo de su represión?

Para muchos esta reacción parecía respaldada por un cierto tipo de liberalismo. Si se dejaba reinar al mercado sin interferencias estatales, la libertad y la prosperidad crecerían inevitablemente y las cosas se solucionarían por sí solas. Ni era necesaria ni tenía cabida una regulación amplia por parte del Estado.

Pero las cosas no se solucionaron por sí solas y los mercados tampoco florecieron. Los estados se encontraban atrofiados y un estado atrofiado no es ningún elixir de la libertad. Así pues, el poder del Estado no se esfumó sino que pasó a unos mafiosos, que en buena parte había creado el propio Estado. La necesidad de las funciones tradicionales —policía, justicia, educación, sanidad— no desapareció y no surgieron intereses privados que las asumieran. Por lo tanto, dichas funciones simplemente se quedaron sin cubrir. La seguridad se evaporó y una anarquía moderna pero torpe reemplazó al anodino comunismo que vivieron las tres generaciones precedentes; al tiempo que en las calles refulgían los letreros de neón de Nike, los pensionistas eran víctimas de fraudulentas operaciones bursátiles que les despojaban de todos sus ahorros y los banqueros caían asesinados a plena luz del día en Moscú. Un sistema de control había sustituido a otro, y ningún liberal occidental podría llamar a eso «libertad».

A mediados de los noventa, justo cuando comenzaba a declinar la euforia postcomunista, emergió en Occidente otra «nueva sociedad» que muchos consideraron tan apasionante como las nuevas sociedades de la Europa postcomunista. Se trataba de Internet o, como lo definiré más adelante, del «ciberespacio». Primero en las universidades y centros de investigación y, poco después, en la sociedad en general, el ciberespacio se convirtió en un nuevo objetivo de los utópicos liberales. *Aquí* sí que reinaría la libertad al margen del Estado. Si no había sido posible hacerlo en Moscú o en Tiblisi, entonces sería en el ciberespacio donde se forjaría la sociedad liberal ideal.

El catalizador de este cambio resultó igualmente imprevisto. Nacido a partir de un proyecto de investigación del Departamento de Defensa estadounidense,[1] el ciberespacio también surgió del desplazamiento imprevisto de una determinada arquitectura de control. La red telefónica restrictiva y de finalidad única fue desplazada por la red abierta y de finalidad múltiple que se basaba en la transmisión de paquetes de datos. De esta forma, la antigua arquitectura editorial de tipo monodireccional (propia de televisión, radio, prensa y libros) se vio complementada por un mundo donde cualquiera podía convertirse en editor. La gente tenía la posibilidad de comunicarse y asociarse de un modo nunca visto. Este espacio parecía prometer un tipo de sociedad inconcebible en el espacio real —libertad sin anarquía, control sin Estado, consenso sin poder. En palabras de un manifiesto que definía este ideal: «Rechazamos reyes, presidentes y votaciones. Creemos en el consenso general y en el código que funciona».[2]

Tal y como ocurrió en la Europa postcomunista, las primeras concepciones acerca de la libertad en el ciberespacio ligaban ésta a la desaparición del Estado. John Parry Barlow, ex letrista de *Grateful Dead* y cofundador de la EFF (*Electronic Frontier Foundation*, Fundación de la Frontera Electrónica), lo expresó así en su «Declaración de Independencia del Ciberespacio»:

> Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro, os pido a vosotros, que pertenecéis al pasado, que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía allí donde nosotros nos reunimos.

Ahora bien, en este caso se decía que dicha ligazón era aún más fuerte que en la Europa postcomunista. Ya no es que el Estado no fuera a regular el ciberespacio, es que *no podría* aunque quisiera, pues el ciberespacio era indefectiblemente libre por naturaleza. Por mucho que los estados amenazaran, la conducta no podría regularse en él; por más leyes que promulgaran, éstas no surtirían ningún efecto. No cabía elegir qué clase de estado implantar porque en el ciberespacio no podría imperar ninguno. El ciberespacio sería

---

1 Véase Katie Hafner y Matthew Lyon, *Where Wizards Stay Up Late*, Nueva York, Simon and Schuster, 1996, p. 10: «Dentro de la *Advanced Research Projects Agency* del Departamento de Defensa, Taylor había sido el joven director encargado de supervisar la investigación informática. [...] Taylor sabía bien que ARPANET y su sucesora, Internet, no tenían nada que ver con respaldar la guerra o sobrevivir a ella...».

2 Cita de David Clark en Paulina Borsook, «How Anarchy Works», *Wired*, 110, octubre de 1995, núm 3.10, disponible en http://www.wired.com/wired/archive/3.10/ietf.html.

una sociedad plenamente diferente y su definición y dirección serían construidas de abajo a arriba. Dicha sociedad se dotaría a sí misma de orden, sería una entidad limpia de gobernantes y libre de intromisiones políticas.

Durante los primeros veranos de la década de los noventa, estuve impartiendo clases en Europa Central y a través de mis alumnos pude ser testigo directo del cambio de actitud hacia el comunismo que he descrito. He ahí el porqué de que experimentara cierta sensación de *déjà vu* cuando, en la primavera de 1995, mis estudiantes de Derecho del ciberespacio manifestaban las mismas ideas postcomunistas acerca de la libertad y el Estado. Incluso en la Universidad de Yale —no precisamente célebre por su apasionamiento liberal— los alumnos parecían borrachos de lo que James Boyle denominaría después el «sofisma liberal»:[3] que ningún estado podría sobrevivir sin las riquezas de Internet, pero que tampoco podría controlar la vida que allí se producía. Los estados del espacio real se volverían tan patéticos como los últimos regímenes comunistas: estábamos ni más ni menos ante la fulminación del Estado, que Marx había prometido, por medio de una sacudida de trillones de gigabytes que fulguraban a través del éter del ciberespacio.

Sin embargo, en medio de tanto festejo nadie se preocupó de aclarar el *porqué* de tales aseveraciones: ¿Por qué no podía regularse el ciberespacio? ¿Qué lo impedía? La misma palabra alude al control, más que a la libertad. Su etimología va más allá de la novela de William Gibson *Neuromante* (publicada en 1984) para remitir al mundo de la «cibernética», esto es, al estudio del control a distancia.[4] Así que resultaba doblemente chocante contemplar el festejo de la «libertad perfecta» bajo una bandera que apunta (al menos, para quien conozca su origen) al control perfecto.

---

3 James Boyle, intervención en la *Telecommunications Policy Research Conference* (TPRC), Washington DC, 28 de septiembre de 1997. David Shenk discute el liberalismo que inspira el ciberespacio (amén de otros problemas capitales de nuestra era) en un brillante manual cultural que abarca tanto la tecnología como el liberalismo; véase *Data Smog: Surviving the Information Glut*, San Francisco, Harper Edge, 1997, esp. pp. 174–77. El libro también describe el tecnorrealismo, un movimiento de sensibilización que propone una visión más equilibrada de la relación entre la tecnología y la libertad.

4 Véase Kevin Kelley, *Out of Control: The New Biology of Machines, Social Systems and the Economic World*, Reading (Mass.), Addison-Wesley, 1994, p. 119. El término «cibernética» lo acuñó un importante fundador en este ámbito, Norbert Wiener; véase *Cybernetics: Or Control and Communication in the Animal and the Machine*, Cambridge (Mass.), MIT Press, 1961 [1948] [ed. cast.: *Cibernética. O el control y comunicación en animales y máquinas*, trad. por Francisco Martín, Barcelona, Tusquets, 1985]. Véase también Flo Conway y Jim Siegelman, *Dark Hero of the Information Age: In Search of Norbert Wiener, The Father of Cybernetics*, Nueva York, Basic Books, 2004.

Como he dicho, soy un estudioso del Derecho Constitucional, ámbito sobre el que escribo e imparto clases. Y creo que esas primeras ideas sobre el Estado y el ciberespacio iban tan descaminadas como las primeras ideas sobre el Estado en la Europa postcomunista. La libertad en el ciberespacio no emanará de la ausencia de Estado, sino que provendrá, como en cualquier otro sitio, de la existencia de un cierto tipo de Estado. No construimos un mundo en el que la libertad pueda florecer si eliminamos de la sociedad todo control autoconsciente, sino si la asentamos sobre un lugar donde se de un tipo específico de control autoconsciente. Así pues, construimos la libertad como lo hicieron nuestros fundadores, asentando la sociedad sobre una determinada *constitución*.

Con todo, cuando hablo de «constitución» no me refiero a un texto legal; a diferencia de lo que hacían mis compatriotas en Europa del Este a comienzos de los noventa, yo no trato de vender un documento que los fundadores de EEUU escribieron en 1787. Me refiero, más bien, al modo en que los británicos hablan de su «constitución»: una arquitectura —no sólo un texto legal sino un modo de vida— que estructura y constriñe los poderes sociales y legales con el propósito de proteger una serie de principios fundamentales. (Un estudiante me preguntó si empleaba «constitución» en el sentido de «un mero instrumento entre otros muchos, una simple linterna que nos permite no tropezar en medio de la oscuridad o, de otro modo, [...] más bien como un faro al que apelamos constantemente». Yo hablo de constitución como un faro —una guía que ayuda a anclar principios fundamentales).

En este sentido, las constituciones se construyen, no se encuentran. Los cimientos se erigen, no aparecen por arte de magia. Del mismo modo que los fundadores de EEUU aprendieron la lección de la anarquía que siguió a la revolución (no olvidemos que nuestra primera constitución, los Artículos de la Confederación, supuso un fracaso marcado por la desidia), también nosotros comenzamos a entender que en el ciberespacio esa construcción, ese fundamento, no es obra de una mano invisible. No hay razón para creer que los cimientos de la libertad en el ciberespacio emergerán como si tal cosa; es más, la pasión por aquella anarquía se ha desvanecido —como sucedió en EEUU a finales de los años ochenta del siglo XVIII y en el bloque del Este a finales de los noventa del siglo pasado. Como los fundadores aprendieron y como los rusos han visto, tenemos razones de sobra para pensar que si abandonamos el ciberespacio a su suerte, éste nunca cumplirá su promesa de libertad. Abandonado a su suerte, el ciberespacio se convertirá en una herramienta de control perfecta.

Control. No necesariamente un control estatal, tampoco necesariamente un control con un fin pérfido, fascista. Lo que defiende esta obra es que la mano invisible del ciberespacio está construyendo una arquitectura diametralmente opuesta a la arquitectura original de dicho espacio. Dicha mano invisible, espoleada por el Estado y por el comercio, está edificando una arquitectura que perfeccionará el control y permitirá una regulación altamente eficaz. En ese mundo la lucha no atañerá al Estado, sino que implicará asegurar que se preserven las libertades esenciales en este entorno de control perfecto. Como afirma Siva Vaidhyanathan:

> Pese a que alguna vez pareció obvio declarar el ascenso de una «sociedad en red» en la que los individuos se reorganizarían, se harían fuertes y socavarían los métodos tradicionales de control social y cultural, hoy parece claro que la comunicación digital en red no tiene por qué servir a esos fines de liberación.[5]

Este libro trata de la metamorfosis de un ciberespacio de anarquía en un ciberespacio de control. Observando la trayectoria actual del ciberespacio —una evolución que describo en la Primera Parte—, es fácil ver que buena parte de la «libertad» presente en su fundación será eliminada de su futuro, que los principios originariamente fundamentales no sobrevivirán. Esa trayectoria que hemos elegido nos llevará a reformar lo que era el ciberespacio en un principio. Ciertas reformas gustarán a muchos, pero todos deberíamos lamentar algunos otros cambios.

No obstante, tanto si las celebramos como si no, resulta crucial comprender cómo ocurrieron. ¿Qué produjo la «libertad» del ciberespacio y qué cambiará al reformarla? Esta reflexión llevará a otra acerca de la fuente de regulación en el ciberespacio.

Alcanzar tal comprensión es el propósito de la Segunda Parte. El ciberespacio exige una comprensión novedosa de cómo funciona la regulación y, así, nos compele a mirar más allá del ámbito tradicional de los abogados —más allá de las leyes o incluso de las normas. El ciberespacio requiere una concepción más amplia de la «regulación» y, lo que es más importante, el reconocimiento de un regulador de singular relevancia.

---

5 Siva Vaidhyanathan, «Remote Control: The Rise of Electronic Cultural Policy», *Annals of the American Academy of Political and Social Science*, vol. 597, núm. 1, 1 de enero de 2005, p. 122.

Dicho regulador es la oscuridad que da título a este libro —el código. En el espacio real, somos capaces de reconocer de qué modo reglamentan las leyes —por medio de constituciones, estatutos y demás códigos legales. En el ciberespacio, hemos de comprender cómo regula un «código» diferente —esto es, cómo el software y el hardware, que hacen del ciberespacio lo que es, constituyen su «código». Como subraya William Mitchell, dicho código es la «ley» del ciberespacio.[6] Joel Reidenberg la denominó *Lex Informatica*,[7] si bien prefiero la fórmula «el código es la ley».

No obstante, hay abogados y teóricos legales que se molestan cuando repito este eslogan. Existen diferencias, insisten, entre los efectos reguladores producidos por el código y los determinados por la ley, no siendo la menor de ellas la referida a la «perspectiva interna» que atañe a cada tipo de regulación. Comprendemos la perspectiva interna de la regulación legal —por ejemplo, que las restricciones que la ley pudiera imponer a la «libertad para contaminar» de una empresa son producto de una regulación autoconsciente, que refleja los valores de la sociedad que impone dicha norma. Ahora bien, dicha perspectiva resulta más difícil de reconocer con el código, donde quizá pueda encontrarse, pero no necesariamente. Y no cabe duda de que ésta no es más que una de las muchas diferencias importantes entre el «código» y la «ley». No pretendo negar estas diferencias, sólo afirmo que podemos aprender algo útil si las ignoramos por un instante. Es célebre la teoría del juez Holmes que asume como núcleo de la regulación la existencia del «mal hombre».[8] Para Holmes, no se trataba tanto de pensar que todos y cada uno de nosotros fuéramos ese «mal hombre», sino de encontrar el mejor modo de construir sistemas de regulación.

Lo mismo ocurre en mi caso. Lo que sugiero es que podemos aprender algo si nos planteamos la teoría de la regulación del «hombre robot»[9]– la cual se centra en la regulación del código. En otras palabras, aprenderemos

---

6 Véase William J. Mitchell, *City of Bits: Space, Place, and the Infobahn*, Cambridge (Mass.), MIT Press, 1995, p. 111. Buena parte de este libro se basa en el planteamiento de Mitchell, aunque la metáfora la tomé también de otros autores. Ethan Katsh discute la noción de mundos de software en «Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace», *University of Chicago Legal Forum*, 1996, pp. 335, 338. El esfuerzo actual más destacado en este sentido es el de R. Polk Wagner, «On Software Regulation», *Southern California Law Review*, núm. 78, 2005, pp. 457, 470–71.

7 Joel Reidenberg plantea la noción relacionada de «lex informatica» en «Lex Informatica: The Formulation of Information Policy Rules Through Technology», *Texas Law Review*, núm. 76, 1998, p. 553.

8 Oliver Wendell Holmes Jr., «The Path of the Law», *Harvard Law Review*, núm. 10, 1897, p. 457.

9 Lessig introduce aquí un juego de palabras entre su *bot man* (donde la partícula *bot* proviene de la abreviatura de «robot») y el *bad man* («mal hombre») del juez Holmes. [N. del E.]

algo importante si imaginamos el objetivo de la regulación como una entidad de maximización, y a partir de ahí consideramos qué gama de herramientas tenemos para controlar esa máquina.

El código será una herramienta capital de este análisis, pues representará la mayor amenaza tanto para los ideales progresistas como para los liberales, a la vez que su mayor promesa. Así pues, nos enfrentamos a la siguiente disyuntiva: podemos construir, diseñar o *codificar* el ciberespacio para proteger principios que juzgamos fundamentales; o bien podemos construir, diseñar o codificar el ciberespacio para dejar que desaparezcan. No hay un punto medio, no nos queda más remedio que optar por uno u otro tipo de construcción. Y ello porque el código no viene dado, sino que tiene que elaborarse, hemos de elaborarlo nosotros, tal y como apunta Mark Stefik: «Las diferentes versiones [del ciberespacio] favorecen tipos diferentes de sueños. A nosotros nos corresponde, sabiamente o no, elegir».[10] En otras palabras, el código «determina quiénes podrán acceder a qué objetos digitales [...]. El modo en que dicha programación regule las interacciones humanas [...] dependerá de la opción que se tome».[11] O, para ser más precisos, ya queda fuera de discusión el hecho de que se va a desarrollar un código y que éste definirá las libertades y el control en el ciberespacio. La única elección que podemos tomar es quién lo construirá y con qué principios.

Mi propuesta no está a favor de formas de control de arriba abajo; tampoco de que los reguladores invadan Microsoft. Una constitución imagina un entorno y, como dijo el juez Holmes, «trae al mundo a un ser cuyo desarrollo no puede preverse». Por consiguiente, hablar de una constitución no implica describir un plan de aquí a cien días, sino identificar los principios que debe garantizar un espacio. Tampoco implica describir un «Estado»; ni tan siquiera elegir (como si debiera hacerse una única elección) entre el control de abajo a arriba y el de arriba a abajo. Hablar de una constitución para el ciberespacio supone simplemente preguntarse: ¿qué principios deberían protegerse? ¿Qué principios deberíamos infundir en este espacio para impulsar determinadas formas de vida?

Los «principios» que están en juego aquí son de dos clases —sustantivos y estructurales. La tradición constitucional estadounidense se ha venido preocupando más por los segundos que por los primeros. Los padres de la Constitución de 1787 (promulgada sin una Declaración de Derechos) se centraron en las

---

10 Mark Stefik, «Epilogue: Choices and Dreams», en *Internet Dreams: Archetypes, Myths, and Metaphors,* Mark Stefik (ed.), Cambridge (Mass.), MIT Press, 1996, p. 390.

11 Mark Stefik, *The Internet Edge: Social, Technical, and Legal Challenges for a Networked World*, Cambridge, MIT Press, 1999, p. 14.

estructuras del Estado. Su propósito era asegurar que un gobierno en particular (el gobierno federal) no acumulara demasiado poder, por lo que introdujeron en el diseño de la Constitución mecanismos que controlaran el poder del gobierno federal y limitaran su alcance sobre los diferentes estados.

Los opositores al documento insistían en que dichos mecanismos no bastaban, y en que la Constitución debía imponer límites sustantivos al poder del Estado, además de los estructurales. Y así nació la Declaración de Derechos que, ratificada en 1791, prometía que el gobierno federal no conculcaría una serie de libertades —libertad de expresión, privacidad y derecho a un juicio justo—, al tiempo que garantizaba que el compromiso con estos principios sustantivos perduraría por encima de los caprichos pasajeros de los distintos gobiernos. Tales principios —tanto sustantivos como estructurales— quedaron, pues, consolidados en nuestro diseño constitucional, y sólo podrían modificarse mediante un proceso largo y costoso.

Con respecto a la constitución del ciberespacio, nos enfrentamos a las mismas preguntas, si bien nos hemos aproximado a ellas desde una dirección opuesta.[12] La lucha referida a los derechos sustantivos ya ha comenzado: ¿prometerá el ciberespacio privacidad o acceso? ¿Permitirá una cultura libre o una cultura del permiso? ¿Preservará un espacio para la libertad de expresión? He aquí una serie de elecciones referidas a los principios sustantivos, sobre los cuales se hablará en profundidad en este libro.

Ahora bien, la estructura también importa, por más que ni siquiera hayamos comenzado a comprender cómo limitar, o reglamentar, el poder regulador arbitrario. ¿Qué mecanismos de control y equilibrio son posibles en este espacio? ¿Cómo separar los poderes? ¿De qué manera se asegura que un regulador, o un Estado, no acapare demasiado poder ni que tampoco le falte?

Los teóricos del ciberespacio vienen discutiendo todas estas cuestiones desde su mismo nacimiento;[13] pero, como cultura no hemos hecho más que empezar a entenderlo. A medida que nos vamos dando cuenta de cómo nos

---

12 *Missouri vs. Holland,* 252 US 416, 433 (1920).

13 Este debate no es nuevo en la democracia estadounidense. Véase Merritt Roe Smith y Leo Marx (eds.), *Does Technology Drive History?: The Dilemma of Technological Determinism*, Cambridge, MIT Press, 1994, pp. 1–35 («Llevado al extremo, a Jefferson le preocupaba que el proceso civilizador de las tecnologías a gran escala y la industrialización pudieran resultar fácilmente corrompidos y arrastraran consigo la moral y la política económica que mucho les había costado levantar tanto a sus compatriotas como a él») [ed. cast.: *Historia y determinismo tecnológico*, trad. por Esther Rabasco Espáriz y Luis Toharia Cortés, Madrid, Alianza Editorial, 1996].

afectan diferentes estructuras en el seno del ciberespacio —cómo su arquitectura, en el sentido en que la definiré más abajo, nos «regula»—, comenzamos a preguntarnos cómo deberían definirse. La primera generación de estas arquitecturas fue erigida por un sector no comercial —investigadores y hackers colaborando para construir una red; la segunda ha sido edificada por el comercio; y la tercera, aún en fase de diseño, podría muy bien provenir del Estado. ¿Qué regulador preferimos? ¿Cuáles deberían ser controlados? ¿Cómo puede la sociedad ejercer tal control sobre entidades que a su vez aspiran a controlarla?

En la Tercera Parte, retomo estas cuestiones desde el nivel más elemental. Así, contemplo tres áreas en controversia —propiedad intelectual, privacidad y libertad de expresión— e identifico los principios que el ciberespacio modificará en cada una de ellas. Dichos principios son producto de la interacción entre la ley y la tecnología, interacción que a menudo es contraria a la intuición. Mi propósito en esta parte es examinar dicha interacción, de modo que se pueda mapear un modo de preservar los principios que consideramos importantes en cada contexto, sirviéndonos de las herramientas explicadas en la Segunda Parte.

La Cuarta Parte traslada dichas cuestiones al plano internacional, ya que si el ciberespacio es universal, entonces sus pobladores proceden de todo el mundo. Pues bien, ¿cómo convivirán las soberanías de todo el mundo con la reivindicación de «soberanía» del ciberespacio? En este punto esbozaré una respuesta concreta que me parece inevitable y que contribuirá a reforzar la conclusión de la Primera Parte.

En cuanto a la parte final, la Quinta Parte, se trata de la más oscura. La lección central de esta obra es que el ciberespacio requiere que decidamos. Algunas de estas decisiones son, y así deben ser, privadas: ¿Todos los autores quieren imponer copyright a sus obras? ¿Cómo desea proteger su privacidad un ciudadano? Otras, en cambio, implican principios que son colectivos. Finalmente, me pregunto si nosotros —los estadounidenses— estamos preparados para afrontar el desafío que estas decisiones implican. ¿Somos capaces de responder racionalmente, esto es, somos capaces de responder sin incurrir en una pasión indebida o irracional y, por otra parte, contamos con instituciones competentes para comprender y responder a esas decisiones?

Me da la sensación de que la respuesta, al menos por ahora, es negativa. Nos hallamos en una etapa de nuestra historia en que necesitamos urgentemente tomar decisiones fundamentales acerca de nuestros principios básicos,

decisiones que no deberíamos poner en manos de ninguna institución de gobierno. Los tribunales no pueden tomarlas porque nuestra cultura legal no aprueba que ellos diriman las disputas que afectan a principios. El Congreso no debería, porque nuestra cultura política nos lleva a ser profundamente escépticos (y con razón) con respecto a los productos de los gobiernos. Hay mucho de lo que sentirse orgullosos en nuestra historia y en nuestras tradiciones, pero el Estado que tenemos hoy es un fiasco y no deberíamos confiar a su control nada importante, por más que de hecho controle todo lo importante.

El cambio, con todo, es posible, y no me cabe duda de que nos aguardan nuevas revoluciones en el futuro. Lo que me asusta es la enorme facilidad con que el Estado, u otras instancias con intereses poderosos, pueden neutralizar estas revoluciones y el hecho de que se jueguen demasiado como para permitir que se produzca ese cambio real. Nuestro Estado ya ha criminalizado la ética en que se funda el movimiento de software libre, tergiversando el significado de hacker para que designe algo completamente distinto a su sentido original. Junto a ello, el extremismo de la regulación de copyright criminaliza igualmente la creatividad radical que esta red podría generar. Y esto no es más que el principio.

Las cosas podrían ser diferentes. De hecho, son diferentes en otros lugares. Sin embargo, no veo de qué forma podrían ser diferentes para nosotros en este momento. Qué duda cabe que esto no es más que una confesión de los límites de mi propia imaginación, por lo que quedaría muy agradecido a quien me demuestre que estoy en un error. Asimismo, me encantaría ver que somos capaces de volver a aprender —tal y como lo están haciendo los ciudadanos de las antiguas repúblicas comunistas— a escapar de las atróficas ideas acerca de las posibilidades de gobierno. Sea como fuere, nada en la última década, y mucho menos en el último lustro, me ha convencido de que mi escepticismo acerca de la gobernabilidad fuera muy equivocado. Es más, los acontecimientos no han hecho más que acentuar mi pesimismo.

2. Cuatro rompecabezas desde el ciberespacio

Todos los lectores de este libro han utilizado alguna vez Internet; algunos, además, han estado en el «ciberespacio». Internet no es más que el medio por el que enviamos correos electrónicos y publicamos páginas web; la herramienta con la que encargamos libros en Amazon o consultamos los horarios del cine en los sitios de venta de entradas. Google está en Internet, como lo están también las «páginas de ayuda» de Microsoft.

El «ciberespacio», sin embargo, es algo más. Por más que hunda sus raíces en la red, supone una experiencia más rica: nos «internamos» en el ciberespacio atraídos por la intimidad de la mensajería instantánea o el bullicio de los «juegos *online* para múltiples jugadores» (MMOG, por sus siglas en inglés; o bien MMORPG, si se trata de juegos de rol). Algunos creen estar en una comunidad cuando se hallan en el ciberespacio; otros confunden su existencia allí con sus propias vidas. Está claro que la línea que separa el ciberespacio de Internet es sutil, pero existe una importante diferencia experiencial entre ambos. Quienes ven Internet como una especie de gigantescas Páginas Amarillas no comprenderán de qué hablan los ciudadanos del ciberespacio. Para ellos, el «ciberespacio» simplemente es un misterio.

Se trata, en parte, de una diferencia generacional. La mayoría de los que hemos rebasado la cuarentena reconocemos la existencia de Internet, pero no así la del «ciberespacio», pues no llevamos una vida *online* que merezca el calificativo de vida en el «ciberespacio». Para nuestros hijos, en cambio, el ciberespacio supone cada vez más una segunda vida. Millones de jóvenes pasan varias horas al día en los mundos alternativos del ciberespacio —más

adelante nos centraremos en uno de ellos, el juego *Second Life*.[1] Por lo tanto, aunque nos digamos que nos da igual ese extraño espacio que nunca llegaremos a visitar, más nos valdría dedicar un tiempo a comprenderlo si es que pretendemos hacernos una idea del mundo que habitará la próxima generación.

A este propósito responden dos de los siguientes relatos, donde se describe el ciberespacio. Los otros dos se ocupan de un modo más general de ciertos aspectos de Internet. Con estas cuatro historias tan diferentes aspiro a desorientar un poco al lector para poder situarle mejor y que llegue así a comprender cuatro temas recurrentes a lo largo de la obra. Al final de este segundo capítulo desvelaré al lector cuáles son estos temas y le proporcionaré una guía; pero centrémonos ahora en los relatos.

Límites

Nada había de extraordinario en la disputa entre Martha Jones y sus vecinos;[2] era la típica discusión que los vecinos siempre han tenido, no desencadenada por un enfado, sino por un malentendido. Y es que en este mundo los malentendidos resultan de lo más común. En eso pensaba Martha mientras se preguntaba si debía permanecer allí; había otros barrios adonde podría ir. Marcharse supondría abandonar cuanto había construido, pero esas frustraciones estaban comenzando a hacerle mella. Quizá había llegado la hora de mudarse, se dijo.

La disputa era acerca de los límites —acerca de dónde acababa su terreno. Parecía algo muy simple, una de esas cuestiones que cualquiera pensaría que las autoridades pertinentes habrían zanjado hace muchos años. Pero ahí estaban su vecino Dank y ella, discutiendo una vez más sobre los límites; o, más bien, sobre algo borroso relacionado con ellos —algo de Martha que invadía el terreno de sus vecinos. El origen de la disputa era algo que Martha había hecho.

---

1 Second Life— «What is Second Life?» disponible en http://secondlife.com/whatis/. El juego que triunfa en la actualidad, *World of Warcraft*, afirma contar con más de 5 millones de suscriptores. Disponible en http://www.blizzard.com/press/051219.shtml.

2 La disputa es hipotética. He construido esta historia basándome en lo que podría pasar y, en ciertos lugares, de hecho, pasa. Al fin y al cabo, soy un profesor de Derecho: me gano la vida construyendo hipótesis.

Martha cultivaba flores, pero no unas flores cualesquiera, sino unas con un extraño poder; eran hermosas y extasiaban con su perfume, sí, pero también eran venenosas. Éstas eran las ocurrencias de Martha: cultivar flores de extraordinaria belleza, pero letales para quien las tocara. Algo sin duda extravagante, pero nadie dijo que Martha no fuera extravagante: era rara, como su vecindario. Lamentablemente, lo que no era raro allí eran estas peleas.

El inicio de la discusión era más que predecible. El perro de Dank murió tras comer un pétalo de las flores de Martha. Un pétalo hermoso que acababa de matar a un perro. Dank tenía sus ideas sobre las flores y sobre el barrio, y no se cortó un pelo al expresarlas —quizá con demasiada exaltación o quizá con la exaltación propia de la situación.

«¡No hay ninguna razón para cultivar flores venenosas!», bramó Dank a través de la valla. «Tampoco la hay para ponerse así por un puñado de perros muertos», replicó Martha. «Un perro siempre se puede sustituir. Y, a fin de cuentas, ¿por qué tienes un perro que sufre cuando se muere? Consigue un perro que muera sin sufrimientos y así mis pétalos no le harán ningún daño».

Yo me encontré con la discusión más o menos en este punto. Pasaba por allí del modo en que uno *pasa por allí* en este espacio (previamente me había teletransportado, pero no conviene complicar la historia con jerga especializada; digamos sólo que pasaba por allí) y vi a los dos vecinos cada vez más enfurecidos el uno con el otro. Yo había oído algo acerca de las flores de la discordia y de sus pétalos venenosos y me pareció un problema fácil de resolver; supongo que estos problemas sólo son fáciles de resolver si se llega a comprender cómo surgen.

Dank y Martha estaban enfadados porque en cierto sentido estaban bloqueados. Ambos habían invertido muchas horas en la construcción de sus vidas en ese vecindario, pero ahora comenzaban a percibir sus límites. Esto es algo de lo más habitual: todos construimos nuestras vidas en lugares con límites, y a veces nos llevamos disgustos. ¿Qué tenía, pues, de diferente la historia de Dank y Martha?

Una diferencia era la naturaleza del espacio, o contexto, donde tenía lugar su disputa, pues no se trataba de un «espacio real», sino de un espacio virtual que formaba parte del llamado «ciberespacio». Dank y Martha se encontraban en un «juego *online* para múltiples jugadores» (MMOG) y un espacio MMOG se diferencia bastante del que llamamos real.

El espacio real es el lugar donde se encuentra el lector en este preciso instante: su oficina, su estudio, acaso una piscina. Se trata de un mundo definido tanto por leyes que han creado las personas como por otras ajenas a ellas. La «responsabilidad limitada» de las sociedades es un ejemplo de ley creada por las personas e implica que, por regla general, a los directores de una empresa no se les puede considerar personalmente responsables de las infracciones de ésta. La vida limitada de los humanos no es una ley que nosotros hayamos creado: nada tiene que ver el Congreso con el hecho de que todos moriremos algún día. En el espacio real, nuestras vidas están sujetas a ambos tipos de leyes y, en principio, sólo nos está dado cambiar uno de ellos.

Pero éstos no son los únicos tipos de leyes del espacio real. El lector habrá comprado este libro, espero, o se lo habrá pedido prestado a alguien que lo hizo. Si lo ha robado, entonces es un ladrón, le pillen o no. Nuestro lenguaje constituye una norma y las normas se determinan colectivamente. En este caso, nuestras normas determinan que ese «robo» convierte al lector en un ladrón, y no sólo porque se llevara el libro. Hay infinidad de maneras de llevarse cosas sin ser considerado un ladrón. Así, si el lector se encuentra un dólar por la calle y lo coge, eso no le convierte en ladrón; es más, si no lo coge, podrían llamarle necio. Ahora bien, robar este libro de la librería (por más que queden muchos otros para los demás) le marca como un ladrón, porque así es cómo funcionan las normas sociales y vivimos sujetos a ellas.

Algunas de estas normas pueden modificarse colectivamente, pero no de forma individual. Puedo decidir prender fuego a mi cartilla de alistamiento, pero no decidir si eso me convertirá en un héroe o en un traidor. Puedo rechazar una invitación a almorzar, pero no decidir si esto será considerado una grosería. La vida real nos plantea muchas opciones, pero no la de escapar a las consecuencias de dichas opciones. En este sentido, las normas nos constriñen de manera tan cotidiana que nos resultan invisibles.

El espacio MMOG es diferente. En primer lugar, se trata de un espacio virtual —como los dibujos animados que vemos en televisión, a veces diseñados en 3D. Ahora bien, a diferencia de los dibujos animados, el espacio MMOG nos permite controlar a los personajes que aparecen en pantalla en tiempo real; o, al menos, nos permite controlar a nuestro personaje —uno de los muchos personajes controlados por otras muchas personas en este espacio. De este modo, construimos el mundo donde vamos a habitar. De niños, crecimos aprendiendo las leyes físicas que gobernaban el mundo del Correcaminos y el Coyote (violento, sí, pero clemente); sin embargo, nuestros hijos crecerán construyendo el mundo del Correcaminos y el Coyote

(también violento, pero quizá no tan clemente). Ellos definirán el espacio y a continuación desarrollarán en él su historia. Sus decisiones crearán las leyes de ese espacio.

Esto no implica que el espacio MMOG sea irreal: en él hay vida real, constituida por los modos en que la gente interactúa. El «espacio» describe el lugar donde la gente se interrelaciona —en buena medida, sin duda, como lo hace en el espacio real, pero con ciertas diferencias significativas. En el espacio MMOG la interacción se da en un medio virtual, «en» el ciberespacio. La gente «se zambulle» en estos espacios virtuales y realiza cosas; y al decir «gente» hablamos de millones de personas. Según Edward Castronova, «una cifra absolutamente mínima sería 10 millones [aunque] mi estimación oscila entre 20 y 30 millones» de personas conectadas a estos mundos virtuales.[3] El «usuario típico pasa entre 20 y 30 horas a la semana dentro de esta fantasía. Los usuarios avanzados pasan allí todo el tiempo que pueden».[4] Un estudio calcula que, «asumiendo un tiempo medio de contacto entre estos 9,4 millones de personas, los suscriptores de mundos virtuales podrían estar consagrando 213 millones de horas semanales a construir sus vidas virtuales».[5]

Las cosas que la gente realiza en estos mundos son muy variadas. Algunos se dedican a los juegos de rol: trabajan en el seno de un grupo de jugadores para acrecentar su estatus y su poder con el fin de alcanzar su objetivo final. Hay quienes simplemente se reúnen para chismorrear: aparecen (bajo la forma que seleccionan y con cualidades y biografías inventadas) en una sala virtual y se intercambian mensajes. Otros se dan una vuelta (de nuevo la ambigüedad resulta notable) y hablan con la gente. Mi amigo Rick lo hace bajo la apariencia de un gato —un gato macho, recalca— y, como tal, Rick se pasea por este espacio y charla con quienquiera que encuentre interesado. Su objetivo es encontrar amantes de los gatos; al resto de gente se limita a castigarla, según cuenta.

Otra gente hace mucho más que chismorrear. Hay, por ejemplo, quien se establece allí. En función del mundo y de sus leyes, los ciudadanos reciben o compran parcelas de terreno sin explotar y dedican una extraordinaria

---

3 Edward Castronova, *Synthetic Worlds: The Business and Culture of Online Games*, Chicago, University of Chicago Press, 2005, p. 55.

4 *Ibid*., p. 2.

5 John Crowley y Viktor Mayer-Schoenberger, «Napster's Second Life?—The Regulatory Challenges of Virtual Worlds», Kennedy School of Government, Documento de Trabajo núm. RWP05–052, 2005, p. 8.

cantidad de tiempo a construir una vida en ellas. (¿No es increíble cómo pierde el tiempo la gente? Mientras nosotros nos pasamos el día trabajando para empresas que no son nuestras y construyendo futuros que no sabemos si llegaremos a disfrutar algún día, esta gente se dedica a diseñar y construir cosas y a crearse una vida, aunque sólo sea virtual. ¡Qué escándalo!). En esas parcelas levantan sus casas —las diseñan y luego las construyen— e invitan a familiares o amigos, se entregan a sus aficiones o crían mascotas. También hay quien cultiva árboles o extrañas plantas, como las de Martha.

El espacio MMOG surgió de la expansión de los espacios MUD o MOO,[6] que también son mundos virtuales pero basados en texto. En ellos no hay elementos gráficos, tan sólo textos que cuentan lo que alguien hace o dice. Podemos construir objetos en un espacio MOO y ponerlos a hacer cosas, pero siempre por mediación de textos. (Sus acciones son, por lo general, bastante sencillas, lo que no quita que sean divertidas. Un año, en un MUD que utilicé en una clase sobre ciberderecho, alguien creó un personaje llamado JPosner. Si alguien le incordiaba, JPosner refunfuñaba: «El incordio es ineficaz». Otro personaje se llamaba Feasterbrook y si alguien coincidía con él en una sala y empleaba el término «justo», Feasterbrook repetía la misma frase, sustituyendo «justo» por «eficaz». De este modo, a la frase «no es justo» replicaba «querrás decir que no es eficaz»).

Aunque a la gente aficionada a los textos o a la escritura no le costaba comprender la atracción de estas realidades basadas en texto, para muchos otros que no compartían tal afición no resultaba tan fácil. El espacio MMOG permite en cierto grado superar ese límite, siendo como la versión cinematográfica de una novela del ciberespacio. Podemos construir cosas que permanecen aunque nosotros ya no estemos: podemos construir una casa y

---

6 Las siglas MUD han adquirido distintos significados, pero originalmente provenían de *Multi-User Dungeon* (Mazmorra Multiusuario) o de *Multi-User Domain* (Dominio multiusuario). Un MOO es un «MUD orientado a objetos». El análisis de Sherry Turkle sobre la vida en un MUD o en un MOO, titulado *Life on the Screen: Identity in the Age of the Internet*, Nueva York, Simon & Schuster, 1995 [ed. cast.: *La vida en la pantalla: la construcción de la identidad en la era de Internet*, Barcelona, Paidós, 1997], sigue siendo un clásico al respecto. Véase también Elizabeth Reid, «Hierarchy and Power: Social Control in Cyberspace», en Marc A. Smith y Peter Kollock (eds.) *Communities in Cyberspace*, Nueva York, Routledge, 1999, p. 107 [ed. cast.: *Comunidades en el ciberespacio*, trad. por José María Ruiz Vaca, Barcelona, EDIOUC, 2003]. El padre —o dios— de un MUD llamado LambdaMOO es Pavel Curtis. Véase su relato en «Mudding: Social Phenomena in Text-Based Virtual Realities», en Stefik (ed.), *Internet Dreams*, *op. cit.*, pp. 265–292. Para conocer dos páginas mágicas de enlaces sobre la historia de los MUD, véase Lauren P. Burka, «TheMUDline», disponible en http://www.linnaean.org/~lpb/muddex/mudline.html; y Lauren P. Burka, «TheMUDdex», disponible en http://www.linnaean.org/~lpb/muddex/.

la gente que pase por nuestra calle la verá; podemos invitarles a pasar y conocer nuestras cosas, de modo que vean de qué manera creamos nuestro mundo. Y si el espacio MMOG en cuestión lo permite, la gente puede incluso observar cómo hemos cambiado las leyes del mundo real. Así, por ejemplo, mientras que en el espacio real la gente «resbala y cae» al pisar suelo mojado, en el espacio MMOG que nosotros hemos construido esa «ley» puede no existir, de modo que en nuestro mundo los suelos mojados hagan a la gente «resbalar y bailar».

A día de hoy, el ejemplo más acabado de este tipo de espacios es la extraordinaria comunidad de *Second Life*. En él, la gente construye tanto objetos como comunidades, los avatares alcanzan un asombroso nivel de elaboración y sus dueños pasan cientos de miles de horas fabricando cosas que otros ven y algunos disfrutan. Unos crean ropa o nuevos peinados, otros, aparatos de música; el caso es que los suscriptores de *Second Life* producen cualquier objeto o servicio que el lenguaje de programación permita crear. En el momento de escribir este libro, hay más de 100.000 residentes de *Second Life*, que ocupan cerca de 2.000 servidores alojados en el centro de San Francisco y consumen 250 kilovatios de electricidad para hacer funcionar sus ordenadores —el equivalente de 160 hogares.

Pero volvamos ahora a Martha y Dank. Durante su cruce de reproches —en el que Martha culpó a Dank de tener un perro que moría con sufrimiento—, ambos revelaron el aspecto más asombroso de su MMOG. Lo extravagante de la observación de Martha («¿Por qué tienes un perro que sufre cuando se muere? Consigue un perro que muera sin sufrimientos, y así mis pétalos no le harán ningún daño») debería haber chocado al lector, que quizá haya pensado: «Qué raro que alguien llegue a pensar que la culpa no es de los pétalos venenosos, sino del perro que murió sufriendo». Ahora bien, lo cierto es que, en este espacio, Dank tenía la opción de escoger cómo moriría su perro; acaso no de decidir si el «veneno» podía o no «matar» a un perro, pero sí de escoger si el animal «sufriría» al «morir». Igualmente, Dank tenía la opción de elegir si sería o no posible hacer una copia del perro, de modo que pudiera «resucitarlo» si moría. En el espacio MMOG, estas posibilidades no vienen dictadas por Dios o, mejor dicho, si es Dios quien las dicta, entonces éste comparte su poder con los jugadores. Y es que las posibilidades de un espacio MMOG las determina el código —el software, o la arquitectura, que hace del espacio MMOG lo que es. La pregunta «¿qué pasa si...?» es un enunciado de lógica que afirma una relación que se manifiesta en el código. En el espacio real no disponemos de demasiado control sobre el código, pero en el espacio MMOG, sí.

Por consiguiente, cuando Martha dijo lo que dijo sobre el perro, Dank le dio una respuesta que me pareció obvia. «¿Y por qué tus flores han de seguir siendo venenosas cuando se salen de tu terreno? ¿Por qué no haces que los pétalos sólo sean venenosos dentro de él y que una vez fuera —cuando el viento los lleve hasta mis propiedades, por ejemplo— resulten inofensivos?».

No era mala idea, pero no sirvió de mucho, ya que Martha se ganaba la vida vendiendo plantas venenosas. A otros (no muchos, la verdad, pero alguno había) también les atraía esta idea de arte floral ligado a la muerte. Así pues, hacer que las plantas venenosas sólo lo fueran dentro de la propiedad de Martha no solucionaba nada, a menos que ella estuviera dispuesta a acoger en sus tierras a una pandilla de clientes extravagantes.

No obstante, esa idea sugirió otra. «De acuerdo», dijo Dank, «¿y por qué no haces que los pétalos sean venenosos sólo cuando están en posesión de alguien que los haya "comprado"? Y en caso de que los roben o de que se los lleve el viento, dejas que pierdan su veneno. ¿No crees que así se solventaría nuestra disputa?».

La idea era ingeniosa y no sólo ayudó a Dank, sino también a Martha. Tal y como estaba diseñado, el código de ese espacio permitía el robo.[7] (La gente quiere realidad en ese espacio virtual; ya tendrá tiempo de sobra para

---

7 Este rasgo no sólo no es raro en estos espacios, sino que resulta bastante común, al menos en los juegos de rol. Julian Dibbell me describió una «parábola» que conoció en el *Ultima Online*, y que denomina el «caso de la maza Rompehuesos robada»:

> Recibí dos ofertas de una Rompehuesos, una potente maza para descalabrar monstruos y comencé a negociar a dos bandas. En un momento dado, uno de los vendedores me informó de que alguien había robado su Rompehuesos, así que le respondí: «Vale, pues se la compraré al otro tío. Por cierto, ¿sabes quién te la ha robado?». Y entonces me dijo el nombre del otro tío, con lo que me enfrentaba al dilema de si debía o no comprar material robado a sabiendas. Ante ello, pedí consejo a mi mentor en estos asuntos, un tío que llevaba años haciéndose de oro con la venta de estos artilugios y al que tenía por un tío honesto, ya sabes. Así que de algún modo pensaba, quizá incluso esperaba, que me recomendase pasar del trato, diciendo: «Nosotros no hacemos ese tipo de tratos en este negocio. No lo necesitamos» y blablabla. Pero, en lugar de eso, me respondió: «Bueno, el robo forma parte de la programación del juego, es una de las destrezas que incluye, así que, ¿cuál es el problema?». El hecho de que el código permitiera asaltar casas y practicar las destrezas delictivas robando cosas me hizo seguir adelante y cerrar el trato, si bien no dejaba de pensar: «Vaya, en cierto modo es completamente arbitrario que el código del juego incluya esta capacidad, aunque, si no la incluyera, no sería lo mismo; se habrían buscado otra forma de robar la maza». [...]

El caso es que, en el *Ultima Online*, se entiende de forma muy explícita que el código y las reglas permiten el robo. Para mí, resultaba interesante que el juego tuviera sus zonas turbias. El hecho de que permitiera hacer algo moralmente deshonesto y dejase la decisión en manos del jugador lo convertía en un juego interesante. Si ahora me volvieran a proponer el trato, no sé si compraría el objeto robado. A mí también me han robado en el juego, de acuerdo con las reglas, y me ha sentado como un tiro.

Grabación de audio: entrevista con Julian Dibbell (1 de junio de 2006, incluida en el archivo del autor).

el paraíso cuando llegue). Pero si Martha pudiera modificar ligeramente el código de modo que el robo[8] eliminase el veneno de una planta, entonces dicho «robo» también eliminaría su valor. Tal cambio protegería tanto sus ganancias con las plantas como la vida de los perros de Dank. He ahí una solución que beneficiaría a ambos vecinos —lo que los economistas denominan un pareto superior— y que resultaba tan factible como cualquier otra: bastaba con un mero cambio en el código.

Reflexionemos un momento sobre lo que supone todo esto. El «robo» conlleva (como mínimo) que algo cambia de manos. Sin embargo, en el espacio MMOG la «posesión» no es más que una relación definida por el software que, a su vez, define todo el espacio. Ese mismo código debe también definir las propiedades que dicha posesión conlleva, pudiendo distinguir, como en el espacio real, entre tener un pastel y comérselo; o pudiendo anular tal distinción, de modo que podamos comernos el pastel y que, acto seguido, éste reaparezca mágicamente. En el espacio MMOG, el milagro bíblico de los panes y los peces no es tal milagro.[9]

Por lo tanto, ¿por qué no aplicar la misma solución al problema entre Martha y Dank? ¿Por qué no definir la propiedad de modo que incluya la cualidad de venenoso y de modo que la posesión sin propiedad se convierta en posesión sin veneno? Si el mundo se diseñara así, entonces podría resolverse la disputa entre Martha y Dank sin necesidad de que ninguno de los dos alterara su comportamiento, sino simplemente mediante un cambio en las leyes de la naturaleza que liquidase el conflicto.

Llevamos andado un corto camino dentro de este no tan corto libro, pero lo que voy a decir a continuación puede convertirlo en muy breve (al menos, para el lector). Y es que esta obra trata, lisa y llanamente, del interrogante suscitado por esta simple historia y de la sencillez de la respuesta aparentemente simple que se le ha dado. Se acabaron los espacios MMOG y los avatares: la historia de Martha y Dank es el primer y último ejemplo que incluirá vicisitudes. Ahora bien, este sí es un libro acerca del ciberespacio. Lo que defiendo es que tanto «en

---

8 Únicamente el robo, de modo que si se transfiriera la propiedad con un propósito distinto —por ejemplo, si se vendiera—, ese rasgo no se modificaría.

9 Compárese Susan Brenner, «The Privacy Privilege: Law Enforcement, Technology and the Constitution», *Journal of Technology Law and Policy*, núm. 7, 2002, pp. 123, 160. («Las mesas de billar del ciberespacio no necesitan patas, pues allí no existe la gravedad»), parafraseando a Neal Stephenson, *Snow Crash*, Nueva York, Bantam, 1992, p. 50 («en el Metaverso, las mesas sólo tienen tableros, no patas») [ed. cast.: *Snow Crash*, trad. por Juan Manuel Barranquero Ríos, Barcelona, Gigamesh, 2005].

Internet» como «en el ciberespacio», nos enfrentaremos a los mismos interrogantes que Martha y Dank afrontaron, así como a las mismas preguntas que provocó su solución. Tanto «en Internet» como «en el ciberespacio», la tecnología define el entorno del espacio y nos proporciona un grado de control sobre el funcionamiento de las interacciones mucho mayor que en el espacio real. Los problemas pueden programarse o «codificarse» dentro de la historia y del mismo modo pueden «descodificarse». Y aunque hasta ahora la experiencia nos demuestre que los jugadores no quieren mundos virtuales demasiado alejados del mundo real, lo importante por ahora es que existe la capacidad de hacer dichos mundos diferentes. Tal capacidad es la que origina la pregunta cardinal de esta obra: ¿Qué significa vivir en un mundo donde los problemas pueden descodificarse? Es más, en ese mundo, ¿siempre deberíamos descodificar los problemas, en lugar de aprender a resolverlos o castigar a quienes los causaron?

Lo que convierte estas cuestiones en interesantes para el Derecho no es el espacio MMOG en sí mismo, pues van a aparecer igualmente fuera de los espacios MMOG, MUD y MOO. Los problemas que se dan allí son problemas generales de la red y a medida que nuestras vidas se enreden cada vez más en ella, se harán más y más acuciantes.

No obstante, he aprendido lo suficiente en este ámbito como para saber que un mero argumento no bastará para convencer al lector. (Me he pasado los últimos 12 años hablando de este tema; al menos ya sé lo que no funciona). Habrá lectores que capten la idea: bravo por ellos; pero si otros no lo logran, mi deber es explicársela. Para estos últimos, pues, me serviré de un método más indirecto, que presentará las pruebas como una sucesión de historias que pretenden descubrir y desorientar. No olvidemos que ningún otro era el propósito de este capítulo.

Así pues, permítame el lector que le describa algunos otros lugares y las rarezas que los pueblan.

Gobernadores

Hay un Estado —que llamaremos «Boral»— al que no le gusta que sus ciudadanos caigan en el juego, por más que a la mayoría sí que les guste jugar. Pero el Estado es el jefe, la gente lo ha votado, la ley es como es... Resultado: en Boral el juego es declarado ilegal.

Pero he aquí que aparece Internet, manando a través de conexiones telefónicas o por cable en los hogares de Boral, y que algunos de sus ciudadanos deciden que el juego *online* es «el último grito». Un ciudadano de Boral monta un «servidor» (un ordenador que es accesible en Internet) que proporciona acceso al juego en Internet y el Estado le amenaza: «Cierra tu servidor o te encerramos».

El ciudadano boraliano, con prudencia no exenta de picardía, accede a cerrar su servidor —al menos en el Estado de Boral. No es que haya decidido retirarse del negocio del juego, es que va a volver a la carga desde un servidor alquilado en algún «refugio fiscal», al cual podrá conectarse la gente de Boral para jugar por Internet. He aquí la cuestión fundamental: la arquitectura de Internet (al menos en su versión de 1999) determina que sea irrelevante en qué punto del espacio real se halle el servidor, pues el acceso no depende de la geografía. Tampoco depende de lo listos que sean los corredores de apuestas o del hecho de que el usuario sepa quién posee o administra el servidor real. El acceso del usuario puede realizarse anónimamente a través de páginas que acaban impidiendo prácticamente saber *qué* pasó, *dónde* y a *quién*.

En consecuencia, la Fiscal General del Estado de Boral se enfrenta ahora a un problema grave. Puede que haya logrado desterrar de Boral el servidor ilegal, pero sus ciudadanos siguen jugando igual. Antes de que llegara Internet, habría tenido a un grupo de personas al que castigar —los gerentes de sitios de apuestas ilegales y su clientela—, pero ahora la red vuelve potencialmente impunes a esas personas —como mínimo porque es más difícil averiguar quién gestiona el servidor y quién juega. Para la Fiscal General, el mundo ya no es como era. Al pasarse a Internet, los jugadores acceden a un mundo donde su conducta ya no es *regulable*.

Por conducta «regulable» entiendo simplemente aquélla que puede someterse a regulación. Y lo entiendo en términos relativos, no absolutos —en un lugar y en un momento dados, una determinada conducta será más regulable que en otro lugar y otro momento diferentes. Con la historia de Boral simplemente defiendo que la red hace que el juego sea menos regulable de lo que lo era antes; o, al menos, en un sentido que quedará más claro a medida que avance el relato, que la arquitectura original de Internet hace que la vida sea menos regulable en la red que fuera de ella.

Las comunidades de Jake

Si el lector hubiera conocido a Jake en una fiesta en Ann Arbor (en el caso de que Jake fuera a una fiesta allí), le habría pasado desapercibido;[10] y en el improbable caso de que sí que hubiera reparado en él, probablemente habría pensado: «Éste es el típico empollón aburrido de la Universidad de Michigan que vive asustado del mundo o, al menos, de la gente del mundo».

Nadie se habría figurado que Jake era escritor —un escritor de relatos con cierta fama en su círculo, de hecho—; y que, además, también era un personaje de sus propias historias. Y es que el Jake de los relatos distaba bastante del de la vida «real» —si es que tal distinción se sigue teniendo en pie después de leer sus historias.

Jake escribía relatos sobre violencia —algo de sexo también había, pero sobre todo violencia— que rebosaban odio y, especialmente, misoginia. No era suficiente que se violara a la mujer, había que asesinarla; y nada de asesinarla así sin más, había que hacerlo de un modo particularmente lacerante y tortuoso. Esto constituye, desafortunadamente, un género narrativo; uno del que Jake era un maestro.

En el espacio real, Jake se las había ingeniado para disimular esta inclinación y no era más que uno entre tantos chavales: ordinario, nada llamativo e inofensivo. Pero por más inofensivo que pareciera en el espacio real, su perniciosa escritura adquiría cada vez más fama en el ciberespacio, llegando a publicarse algunos de sus relatos en un grupo de USENET llamado alt.sex.stories.

USENET no es en sí misma una red, al menos no más de lo que puedan serlo los anuncios clasificados de un periódico. Se trata, en sentido estricto, del producto de un protocolo —un conjunto de reglas denominadas *Network News Transfer Protocol* (NNTP, Protocolo de transferencia de noticias en red, en castellano)— de intercambio de mensajes públicamente accesibles. Estos mensajes se organizan en «grupos de noticias» y éstos a su vez se organizan por temas, que son mayoritariamente técnicos, pero que también están relacionados con aficiones y algunos con el sexo. En algunos grupos de noticias se incluyen fotos y videos, pero en otros, como el de Jake, sólo hay relatos.

---

10 Jake Baker fue bautizado como Abraham Jacob Alkhabaz, pero decidió cambiarse el nombre tras el divorcio de sus padres. Véase «Writer Arrested After Sending Violent Fiction Over Internet», *New York Times*, 11 de febrero de 1995, p. 10.

Existen millares de grupos de noticias, cada uno de los cuales alberga cientos de mensajes. Cualquiera con acceso a USENET puede acceder a los mensajes (al menos a los que el administrador quiera que lea), publicar uno o responder a otro ya publicado. Imagínese el lector un tablón público de anuncios donde la gente deja sus preguntas o comentarios, y donde cualquiera puede leerlos y añadir sus propias opiniones. Ahora imagínese 15.000 tablones, cada uno con cientos de «hilos» (argumentos encadenados unos con otros): eso, aglutinado en un solo lugar, es USENET. Ahora imagínese esos 15.000 tablones con sus cientos de hilos colgados en millones de ordenadores repartidos por doquier, de modo que, si se publica un mensaje en un grupo, se añade al tablón correspondiente en todo el mundo: eso, en términos mundiales, es USENET.

Jake, como dije, publicaba sus historias en un grupo llamado alt.sex.stories, donde «alt» alude a la categoría en torno a la que se organiza el grupo. Inicialmente, había siete categorías principales[11] y «alt» se creó como reacción a ellas: mientras que la incorporación de grupos a las siete categorías principales se realiza mediante una votación formal de sus participantes, en «alt» queda en manos de los administradores, que deciden generalmente en función de la popularidad del grupo, siempre que ésta no sea controvertida.

Entre estos grupos, alt.sex.stories goza de cierta popularidad. Como sucede en cualquier espacio de escritura, si los relatos son «buenos» según los criterios del espacio —esto es, si son los que demandan sus usuarios—, obtienen un amplio seguimiento y ganan celebridad.

Desde este punto de vista, el material de Jake era muy valioso. Sus narraciones de secuestros, torturas, violaciones y asesinatos de mujeres eran tan gráficos y repulsivos como exigía el género —y como también exigía la gente de esa índole, entre la que Jake adquirió gran fama. Necesitaban relatos de mujeres inocentes violadas y Jake les suministraba gratuitamente una dosis constante y estable.

Una noche, en Moscú, una chica de dieciséis años leyó una de las historias de Jake y se la enseñó a su padre, quien, a su vez, se la mostró a Richard DuVal, un antiguo alumno de la Universidad de Michigan. DuVal quedó conmocionado por el relato, y le enojó ver que en su encabezamiento aparecía la etiqueta «umich.edu», así que llamó al centro para quejarse.

11 Estas siete categorías son comp, misc, news, rec, sci, soc y talk. Véase Henry Edward Hardy, «The History of the Net, v8.5», 28 de septiembre de 1993, disponible en http://www.eff.org/Net_culture/net.history.txt.

Los responsables de la Universidad de Michigan se tomaron la queja muy en serio[12] y contactaron con la policía, que a su vez contactó con Jake —esposándolo y metiéndolo entre rejas. Allí recibió la visita de un tropel de médicos, alguno de los cuales concluyó que Jake constituía una amenaza para la sociedad. Las autoridades locales compartieron tal diagnóstico, especialmente después de incautarse del ordenador de Jake y descubrir un intercambio de correos electrónicos que mantuvo con un fan canadiense que planeaba una adaptación al mundo real de una de las historias que Jake publicó en el ciberespacio; eso, al menos, es lo que se leía en sus correos. Nadie podía conocer a ciencia cierta las intenciones reales de la pareja. Jake alegó que todo eso era pura ficción, y, en realidad, no se halló ninguna prueba que lo desmintiera.

No obstante, Jake se enfrentó a una acusación federal por proferir amenazas. Jake repuso que sus relatos no eran más que palabras y que éstas estaban amparadas por la Primera Enmienda a la Constitución de EEUU. Un mes y medio después, un tribunal admitió tal argumento y retiró los cargos contra Jake,[13] que retornó a la particular oscuridad que había caracterizado su vida hasta entonces.

Ahora bien, lo que me importa aquí no es si las palabras de Jake Baker están o no amparadas por la Constitución. Me interesa el propio Jake Baker, una persona aparentemente inofensiva en el espacio real, pero completamente libre en el ciberespacio para convertirse en un autor de gran violencia. La gente lo defendía diciendo que era valiente, pero él no se comportaba con «valentía» en el espacio real: Jake nunca expresó su odio en clase, entre amigos o en el periódico escolar; sólo daba rienda suelta a sus perversiones cuando se guarecía en el ciberespacio.

Esto era así en parte por él y en parte por el ciberespacio. Por un lado, a Jake le gustaba difundir relatos de violencia, al menos si podía hacerlo sin dar la cara. El ciberespacio le concedía esa potestad, ya que en él Jake podía ejercer tanto de autor como de editor de su obra. Escribía sus relatos y, en cuanto los terminaba, los lanzaba a unos 30 millones de ordenadores repartidos por el mundo en unos pocos días. Su público potencial duplicaba con creces el de las quince primeras novelas en la lista de *best sellers*, y, aunque no se llevara ningún dinero, la demanda de sus historias era alta. Jake había descubierto un modo de inocular su depravación en las venas de un público al que le habría costado mucho dar con ese material de otra forma. (Ni siquiera la revista *Hustler* publicaría algo así).

---

12 He basado mi descripción de los hechos en el vívido relato que Jonathan Wallace y Mark Mangan incluyen en *Sex, Laws, and Cyberspace*, Nueva York, M&T Books, 1996, pp. 63–81, si bien circulan por la red variaciones de la historia más interesantes (me estoy cubriendo las espaldas).

13 Véase *United States vs. Baker*, 890 FSupp 1375, 1390, EDMich 1995; véase también Wallace y Mangan, *Sex, Laws, and Cyberspace*, *op. cit.*, pp. 69–78.

Qué duda cabe que Jake disponía de otros canales de publicación. Podría haberle ofrecido su obra a *Hustler,* o algo peor. Pero ninguna publicación del mundo real le habría proporcionado una audiencia potencial de millones de lectores que atravesaban países y continentes, culturas y gustos.

Tal alcance era posible por el poder de las redes: cualquiera desde cualquier sitio podía publicar para cualquiera en cualquier otro sitio. Las redes permitían publicar sin ningún filtro, ningún proceso de edición y, acaso lo más importante, sin ninguna responsabilidad. Uno podía escribir lo que le apeteciera, ponerle su firma o no, publicarlo en ordenadores de todo el mundo y, al cabo de unas horas, sus palabras se expandirían por doquier. Las redes eliminaban así la cortapisa más importante de la expresión en el espacio real —la separación entre editor y autor. Publicar en el espacio real alimenta la vanidad, pero sólo los ricos consiguen llegar a una audiencia amplia de ese modo; al resto, el espacio real nos proporciona sólo el acceso que los editores quieran concedernos.

Por consiguiente, el ciberespacio es diferente por el alcance que proporciona y también por el anonimato que permite. El ciberespacio permitió a Jake escapar de las cortapisas del espacio real. Él no «se iba al» ciberespacio mientras escribía sus relatos, en el sentido de que no «abandonaba» Ann Arbor. Pero cuando estaba «allí», podía escapar de las normas de Ann Arbor, se liberaba de las restricciones de la vida real, de las reglas y conocimientos que habían logrado hacer de él un miembro de la comunidad universitaria. Puede que Jake no se sintiera exactamente como en casa; puede que no fuera el chico más feliz. Ahora bien, el mundo de la Universidad de Michigan había logrado apartarle de una vida de psicópata —excepto cuando le daba acceso a la red. En la red, Jake era otra persona.

A medida que Internet ha crecido, ha producido muchas más oportunidades para personajes como Jake —personajes que hacen en el mundo virtual lo que nunca harían en el real. Uno de los juegos MMOG más populares es el *Grand Theft Auto*, donde uno se dedica a perpetrar crímenes. Y uno de los usos más turbios del *videochat* es la práctica de la prostitución infantil virtual. Recientemente, el *New York Times* dio la noticia de que millares de niños pasaban cientos de horas prostituyéndose en la red. Sentados en la «intimidad» de su dormitorio, usando la *webcam* que sus padres les regalaron en Navidad, chicas y chicos de 13 años representan las conductas sexuales que demanda su público. De resultas, el público se lleva su dosis de perversión sexual y el crío se lleva su dinero, más todo el lastre psicológico que acarrea tal comportamiento.[14]

---

14 Véase Kurt Eichenwald, «Through His Webcam, a Bot Joins a Sordid Online World», *New York Times*, 19 de diciembre de 2005, A1.

Resulta imposible contemplar esta galería de personajes de pesadilla sin pensar que, en cierta medida, el mundo virtual ha traspasado la frontera de lo real; o, como mínimo, que tiene efectos reales —bien en quienes viven en él, bien en su entorno.[15] Cuando Jake fue llevado a juicio, muchos defensores de la Primera Enmienda alegaron que sus palabras, por más vívidas que fueran, no traspasaron la frontera de lo real. Qué duda cabe de que existe una diferencia entre escribir sobre violaciones y cometerlas, tal y como existe entre un actor que representa una violación y una persona que viola a otra. Pero estimo que todos coincidiremos en que hay un límite que se franquea en alguna parte cuando nos movemos entre esta galería de personajes de pesadilla. Si una madre permaneciera impasible mientras su hijo se prostituye virtualmente en su dormitorio, no la consideraríamos una defensora acérrima de la libertad de expresión, ni aunque dicha «prostitución» se limitara al relato del niño sobre cómo sufrió acoso sexual en un *chat*.

Sea como fuere, mi intención no es establecer una distinción entre las dobles vidas virtuales que resultan aceptables y las que no. Me limito a constatar que este espacio posibilita una dualidad más acentuada; y que, por más que ésta sea «sólo virtual» y a veces se quede «sólo en palabras», los reguladores del espacio real (ya sean padres o estados) se sentirán obligados a reaccionar. La red permite llevar vidas que antes eran imposibles, inconvenientes o insólitas; y al menos algunas de ellas producirán efectos en las vidas no virtuales —tanto para los que viven en el espacio virtual, como para los que les rodean.

Gusanos que fisgonean

Un «gusano» es un fragmento de código informático que se suelta en la red para que se introduzca en el sistema de ordenadores vulnerables. No se trata de un «virus» porque no se incrusta en otros programas para interferir en su funcionamiento. Se trata de un mero fragmento de código extra que lleva a cabo lo que el programador le dice: podría ser inofensivo y simplemente instalarse en una máquina ajena; o podría ser dañino y corromper archivos, o provocar otros perjuicios que el programador le indique.

---

15 Véase C. Anderson y B. Bushman, «Effects of Violent Video Games on Aggressive Behavior, Aggressive Cognition, Aggressive Affect, Physiological Arousal, and Prosocial Behavior: A Meta-Analytic Review of the Scientific Literature», *Psychological Science* 12 (5), 2001, pp. 353–359, disponible en http://www.psychology.iastate.edu/faculty/caa/abstracts/2000-2004/01AB.pdf. Jonathan L. Freedman, *Media Violence and Its Effect on Aggression*, Toronto, Toronto University Press, 2002.

Imagínese el lector un gusano diseñado para hacer el bien (al menos lo que algunos creen que es «el bien»). Imagínese que el autor del código es el FBI y que el FBI está buscando un documento en concreto, uno propiedad de la NSA (*National Security Agency*, Agencia Nacional de Seguridad). Suponga el lector que se trata de un documento secreto cuya posesión es ilegal a menos que se cuente con la autorización pertinente. Imagínese que, una vez en la red, el gusano pueda penetrar en todos los discos duros y realizar un examen completo: si encuentra el documento de la NSA, enviará inmediatamente un mensaje informando al FBI; si no, se autodestruirá. Finalmente, suponga el lector que el gusano puede hacer todo eso sin «interferir» en el funcionamiento del ordenador en cuestión. Nadie se percataría de su presencia y la única información que revelaría sería si el documento secreto de la NSA está en ese disco duro.

¿Estamos ante un gusano inconstitucional? Se trata de una pregunta compleja que en principio parece tener una contestación fácil. El gusano está inmerso en una operación estatal de registro de discos duros de los ciudadanos, sin que (tal y como exige ordinariamente la ley) exista la sospecha razonable de que el documento en cuestión se halle en dichos discos. Estamos, pues, ante un registro estatal arbitrario e injustificado de espacios privados.

Desde el punto de vista de la Constitución —más concretamente de la Cuarta Enmienda—, estamos ante una flagrante violación de la ley. La Cuarta Enmienda se promulgó precisamente para erradicar este tipo de abusos. En el siglo XVIII los reyes británicos Jorge II y Jorge III concedieron a sus oficiales una «orden general» que les autorizaba al allanamiento de morada indiscriminado en busca de pruebas delictivas.[16] Provistos de esa orden, los oficiales podían poner patas arriba la casa de cualquier ciudadano que se les antojara, sin que éste pudiera denunciar tal atropello. El propósito de la Cuarta Enmienda era exigir que existieran sospechas para llevar a cabo un registro, de modo que los ciudadanos sólo tuvieran que padecerlos en determinadas circunstancias razonables.[17]

---

16 Véase William J. Stuntz, «The Substantive Origins of Criminal Procedure», *Yale Law Journal*, núm. 105, 1995, pp. 393, 406–407.

17 Véase, por ejemplo, Thomas K. Clancy, «The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures», *University of Memphis Law Review*, núm. 25, 1995, pp. 483, 632. «La sospecha individualizada [...] ha supuesto un blindaje contra las acciones policiales injustificadas y arbitrarias».

Pero, ¿acaso es equiparable nuestro gusano al registro indiscriminado promovido por la Corona británica? Una diferencia ostensible radica en que, a diferencia de las víctimas de los registros indiscriminados que preocupaban a los padres de la Constitución, las víctimas del gusano nunca se percatan de la intrusión en sus ordenadores. Con los registros indiscriminados, la policía irrumpía en una casa y hurgaba en las cosas de la gente; con el gusano, en cambio, es un fragmento de código el que se desliza en la casa y (hemos supuesto que) sólo puede «ver» una cosa. Más importante aún, a diferencia de los registros indiscriminados, el gusano es discreto y deja todo intacto cuando acaba: el código no puede leer la correspondencia privada, ni echar abajo las puertas; no interfiere, pues, en la vida ordinaria de sus víctimas. Si somos inocentes, no tenemos nada que temer.

El gusano actúa sigilosamente, cosa que no hacían las tropas del rey Jorge. Su registro es implacable pero invisible, delatando sólo a los culpables. El gusano no importuna a la gente inocente, ni a los ciudadanos ordinarios; captura exclusivamente a aquéllos que están fuera de la ley.

Esta diferencia complica la pregunta acerca de la inconstitucionalidad del gusano. El gusano practica un registro indiscriminado en tanto que prescinde de cualquier sospecha previa; pero no es equiparable a los registros indiscriminados clásicos porque no perturba la vida ordinaria de los ciudadanos y sólo «destapa» irregularidades. En este sentido, el gusano es como un perro policía —que, al menos en los aeropuertos, puede olfatear a cualquiera sin necesidad de sospecha previa y bajo el amparo de la Constitución—,[18] pero mejor. A diferencia del perro policía, el gusano ahorra al usuario del ordenador el mal trago que le ocasionaría enterarse de que está siendo registrado.

En ese caso, ¿es el gusano constitucional? Eso depende de nuestra concepción acerca de qué es exactamente lo que salvaguarda la Cuarta Enmienda. Hay quien considera que la Enmienda protege a los ciudadanos de cualquier invasión injustificada por parte del Estado, tanto si les resulta onerosa como si no. Otros, en cambio, aducen que la Enmienda protege a los ciudadanos de las invasiones que les sean molestas, permitiendo sólo aquéllas que cuentan con sospechas fundadas de que se encontrarán elementos incriminatorios. El caso paradigmático que movió a los fundadores a introducir la mencionada Enmienda no contempló tal distinción porque la tecnología de la época no la hacía concebible: ¿Cómo podría —técnicamente— haberse

18 Véase *United States vs. Place,* 462 US 696, 707, 1983.

ejecutado en 1791 un registro indiscriminado que no fuera necesariamente oneroso? Así pues, los fundadores no manifestaron —técnicamente— su concepción acerca de la inconstitucionalidad del registro de nuestro gusano; nos corresponde a nosotros decidir el alcance de la Cuarta Enmienda.

Llevemos un poco más lejos nuestro ejemplo. Imagínese ahora el lector que el gusano no registra todas las máquinas que encuentra a su paso, sino sólo aquéllas que le autoriza una orden judicial: queda así liquidada la cuestión de la necesidad de contar con sospechas previas. Ahora bien, imagínese el lector que esta regla incluye la siguiente cláusula: el Estado exige que las redes informáticas se construyan de modo que permitan instalar en cualquier ordenador un gusano, siempre que medie una autorización judicial. Bajo este régimen, pues, las máquinas habrán de ser *aptas para gusanos*, aunque éstos sólo se introduzcan con un mandato judicial.

Una vez más, ¿existe alguna objeción constitucional ante esto? En el Capítulo 11 exploraré a fondo esta cuestión, así que quedémonos por ahora sólo con su característica más sobresaliente. En ambos casos, estamos describiendo un régimen que permite al Estado recopilar información sobre nosotros de un modo altamente eficaz —que no resulta gravoso ni para el Estado ni para las personas inocentes. Tal eficacia es posibilitada por la tecnología, que permite realizar registros que antes habrían resultado desmesuradamente molestos e invasivos. En ambos casos, pues, la pregunta es la siguiente: si aumenta la capacidad de realizar registros no onerosos, ¿aumenta proporcionalmente el poder del Estado para registrar a los ciudadanos? O, dicho más lóbregamente, en palabras de James Boyle: «¿Es la libertad inversamente proporcional a la eficacia de los medios de vigilancia disponibles?». Porque si es así, en palabras de Boyle, entonces «tenemos mucho que temer».[19]

Esta cuestión, por descontado, no se refiere exclusivamente al Estado. Uno de los rasgos definitorios de la vida moderna es el surgimiento de tecnologías de recopilación y tratamiento de datos extraordinariamente eficaces. La mayor parte de lo que hacemos —y, por ende, la mayor parte de lo que somos— queda registrado fuera de nuestros hogares: cuando llamamos por teléfono, se registra con quién hablamos, cuánto duraron las llamadas y cuándo las hicimos, así como la frecuencia con que se repiten;[20]

---

19 James Boyle, *Shamans, Software, and Spleens: Law and the Construction of the Information Society*, Cambridge (Mass.), Harvard University Press, 1996, p. 4.

20 Véase Susan Freiwald, «Uncertain Privacy: Communication Attributes After the Digital Telephony Act», *Southern California Law Review*, núm. 69, 1996, pp. 949, 951, 954.

cuando pagamos con tarjeta de crédito, se registra cuándo, dónde y a quién compramos qué; cuando viajamos en avión, el Estado registra nuestro itinerario y lo escudriña para determinar la probabilidad de que seamos terroristas;[21] cuando conducimos por el centro de Londres, las cámaras de vigilancia registran nuestra matrícula para determinar si hemos pagado el correspondiente «impuesto de congestión». Sin duda alguna, la imagen hollywoodiense de las unidades antiterroristas —en las que una persona sentada frente a un terminal de ordenador acecha la vida de otra de forma instantánea— es errónea, pero no tiene por qué seguir siéndolo por mucho tiempo. Acaso sea difícil concebir sistemas que sigan a alguien allá donde vaya, pero no lo es tanto imaginar tecnologías que reúnan una ingente cantidad de información sobre todo lo que hacemos y la ponga a disposición de quienes tengan la autorización pertinente. Con un ligero nivel de intrusismo, se obtendría una recompensa suculenta.

En la era digital, pues, tanto el control privado como el estatal tienen la misma destacada característica: el control, o el registro, pueden incrementarse en gran medida sin que resulten más molestos para sus víctimas. Por lo tanto, ambos tipos de control nos plantean una pregunta similar: ¿Cómo deberíamos pensar este cambio? ¿Cómo deberían aplicarse las protecciones que los redactores de la Constitución nos legaron a un mundo que ellos ni siquiera pudieron concebir?

Temas

Cuatro historias, cuatro temas; cada uno de ellos abre una ventana a un aspecto del ciberespacio que será cardinal en todo lo que viene a continuación. Mi objetivo es ir profundizando en dichos temas a lo largo del libro, por lo que concluyo este capítulo ofreciendo un mapa orientativo que los presenta en el orden en que irán apareciendo. Tal orden de aparición nos remite en primer lugar a la segunda historia.

21 Cfr. John Rogers, «Bombs, Borders, and Boarding: Combatting International Terrorism at United States Airports and the Fourth Amendment», *Suffolk Transnational Law Review*, núm. 20, 1997, p. 501, n. 201.

Regulabilidad

Por «regulabilidad» se entiende la capacidad de un Estado de regular la conducta en el ámbito de su jurisdicción concreta. En el contexto de Internet, sería la capacidad del Estado para regular la conducta de sus ciudadanos (como mínimo) mientras están conectados a la red. La historia de Boral trataba, pues, sobre la regulabilidad o, más específicamente, sobre los cambios en la regulabilidad provocados por el ciberespacio. Antes de que existiera Internet, a la Fiscal General de Boral le resultaba relativamente fácil controlar el juego dentro de su jurisdicción; con la llegada de Internet, los servidores se trasladaron fuera de su territorio y la regulación se hizo mucho más difícil.

Para el regulador, esto no es más que un ejemplo particular de una cuestión mucho más general. Y es que para poder regular bien, es necesario saber (1) quién, (2) dónde está y (3) qué está haciendo. Ahora bien, dado el modo en que se diseñó originalmente Internet (volveremos sobre esto más abajo), no había forma alguna de saber (1) quién, (2) ni dónde está (3) ni qué está haciendo. Por consiguiente, a medida que la vida se trasladaba a (esta versión concreta de) Internet, disminuía la regulabilidad que cabía ejercer. La arquitectura del espacio —al menos como era originariamente— volvió la vida en dicho espacio menos regulable.

La Primera Parte de la obra se centra en la regulabilidad: ¿Podemos imaginar un ciberespacio más regulable? ¿Es ése el ciberespacio hacia el que nos dirigimos en este momento?

Regulación por medio del código

La historia de Martha y Dank nos proporciona una pista para responder a estas preguntas. Del mismo modo que en el espacio MMOG podemos alterar las leyes de la naturaleza —haciendo posible lo que antes era imposible y viceversa—, ¿por qué no vamos a poder modificar la regulabilidad en el ciberespacio? En definitiva, ¿por qué no somos capaces de imaginar una red o un ciberespacio donde la conducta pueda controlarse en la medida en que el código lo permita?

A fin de cuentas, el espacio MMOG es, en buena medida, un espacio «regulado», aunque con una regulación muy especial: la que emana del código. En él, las reglas importantes no son impuestas mediante sanciones sociales o normas estatales, sino por medio de la arquitectura misma del espacio en cuestión. Las reglas, pues, no quedan definidas en un estatuto, sino que se inscriben en el código que gobierna el espacio.

He aquí el segundo tema de este libro: la regulación de la conducta en Internet y en el ciberespacio existe y se ejecuta primordialmente mediante el código. En función de las diferencias en la codificación de la regulación, podrán distinguirse diferentes zonas de Internet y del ciberespacio: en algunas, la vida es bastante libre; en otras, está más controlada. Sea como fuere, la diferencia entre dichas zonas es meramente una diferencia en las arquitecturas de control —es decir, una diferencia en el código.

Si combinamos estos dos primeros temas, llegamos a uno de los argumentos centrales de esta obra: la regulabilidad descrita en el primer tema depende del código descrito en el segundo. Algunas arquitecturas del ciberespacio son más regulables que otras; algunas permiten un control más acabado. En consecuencia, de la naturaleza del código dependerá el que se pueda o no regular una zona del ciberespacio —o Internet en su conjunto. Su arquitectura determinará si las conductas se pueden o no controlar; como afirma Mitch Kapor, su arquitectura es su política.[22]

De aquí se deriva que si algunas arquitecturas son más regulables que otras —si algunas proporcionan a los estados mayor control que otras—, entonces los estados favorecerán aquéllas por encima de éstas, ya sea de forma directa o indirecta. De cualquiera de las dos formas, queda claro que las arquitecturas que hacen menos regulable el espacio pueden a su vez ser modificadas para permitir una regulación mayor. (Más adelante nos ocuparemos de quién querría modificarlas y por qué).

---

22 Véase Mitchell Kapor, «The Software DesignManifesto», disponible en http://hci.stanford.edu/bds/1-kapor.html. David Farber, «A Note on the Politics of Privacy and Infrastructure», 20 de noviembre de 1993, disponible en http://www.interesting-people.org/archives/interesting-people/199311/msg00088. html; «Quotations», disponible en http://www.cs.arizona.edu/icon/oddsends/farber.htm. Véase también Pamela Samuelson *et al.*, «A Manifesto Concerning the Legal Protection of Computer Programs», *Columbia Law Review*, núm. 94, 1994, p. 2308. Steven Johnson defiende con contundencia una idea similar: «Toda obra arquitectónica implica una visión del mundo, lo que significa que toda la arquitectura es, en un sentido profundo, política»; véase *Interface Culture: How New Technology Transforms the Way We Create and Communicate*, San Francisco, Harper Edge, 1997, p. 44. La *Electronic Frontier Foundation*, fundada originalmente por Mitch Kapor y John Perry Barlow, ha actualizado el eslogan de Kapor «la arquitectura es política» [*architecture is politics*] convirtiéndolo en «la arquitectura es una medida política» [*architecture is policy*]. Me gustaba más la versión original.

Esta constatación acerca de la regulabilidad constituye una amenaza para aquéllos a los que inquieta el poder estatal y una realidad para quienes lo ostentan. Hay diseños que dotan al Estado de mayor poder que otros y hay diseños que le dotan de poderes distintos. Hemos de elegir entre unos y otros en función de los principios que están en juego.

Ambigüedad latente

El gusano, por su parte, nos habla de una cuestión distinta. Por más que sea una tecnología de registro, nuestro gusano opera de forma diferente a la de los «registros» del espacio real, que acarrean notables costes: son onerosos, pueden generar inseguridad y exponer a sus víctimas a invasiones más allá de lo legítimo.[23] El gusano, en cambio, elimina esos costes: el registro ya no es molesto, es (prácticamente) invisible y su tecnología de rastreo está diseñada para encontrar sólo lo que es ilegal. Esto suscita el interrogante de cómo debería interpretarse un registro tal en términos de constitucionalidad.

Una visión justa de las protecciones de la Constitución podría discurrir por dos vías: se puede contemplar la invasión del gusano como incompatible con la dignidad que la introducción de la Cuarta Enmienda buscaba proteger;[24] o se la puede ver como razonable al ser tan poco invasiva. Ambas respuestas podrían ser válidas, lo que implica que el gusano revela lo que llamo «una ambigüedad latente» en la regla constitucional original. En el contexto original, la regla estaba clara (nada de registros indiscriminados), pero en el actual, la regla depende del principio que la Constitución pretenda proteger. La pregunta queda en el aire y admite (al menos) dos respuestas posibles, en función del valor que se busque proteger. Ahora hemos de elegir una u otra.

---

23 Jed Rubenfeld ha desarrollado más extensamente una teoría interpretativa que basa el significado en una práctica de lectura a través del tiempo, fundada en casos paradigmáticos; véase «Reading the Constitution as Spoken», *Yale Law Journal*, núm. 104, 1995, pp. 1119, 1122; y «On Fidelity in Constitutional Law», *Fordham Law Review*, núm. 65, 1997, p. 1469. Véase también Jed Rubenfeld, *Freedom and Time: A Theory of Constitutional Government*, New Haven, Yale University Press, 2001.

24 Véase *Minnesota vs. Dickerson*, 508 US 366, 380, 1993 (voto coincidente del juez Antonin Scalia: «Dudo francamente [...] que los orgullosos hombres que adoptaron nuestra Cuarta Enmienda hubieran permitido que se les sometiera, bajo la mera sospecha de ir armados y ser peligrosos, a tamaña indignidad...»).

Puede que el lector no se trague mi historia del gusano y piense: «Es pura ciencia ficción». Hacia el final del libro, sin embargo, le convenceré de que existen ciertos casos en los que una ambigüedad similar perturba nuestro pasado constitucional. En muchos de ellos, nuestra Constitución no facilita ninguna respuesta acerca de cómo debería aplicarse, pues al menos existen dos respuestas posibles —a la luz de las decisiones que sus redactores tomaron y dadas las tecnologías contemporáneas.

Tal ambigüedad crea un problema a los estadounidenses. Si en nuestros días los tribunales de justicia se sintieran autorizados para seleccionar el principio que produjera una respuesta más adecuada en el contexto dado, no existiría ningún problema, ya que las ambigüedades latentes quedarían resueltas mediante decisiones judiciales —los redactores podrían haber tomado una u otra vía, pero nuestros jueces resuelven tomar *ésta*.

Pero no vivimos en un momento así, por lo que no disponemos de tribunales que resuelvan tales ambigüedades. De resultas, hemos de confiar su solución a otras instituciones, si bien en este punto mi postura es pesimista: carecemos de dichas instituciones. Si no enderezamos el rumbo, nuestra constitución para el ciberespacio será cada vez más raquítica.

El ciberespacio nos presentará ambigüedades de forma constante y nos presionará para discernir cuál es la mejor respuesta. Hoy en día, disponemos de instrumentos del espacio real que nos ayudarán a resolver las cuestiones interpretativas, orientándonos en un sentido o en otro, al menos algunas veces. Pero tales instrumentos acabarán por orientarnos menos aún de lo que lo hacen en el espacio real. Cuando la brecha entre su orientación y nuestros actos se haga obvia, nos veremos abocados a hacer algo que no se nos da nada bien —decidir lo que deseamos y lo que es correcto.

Soberanos en competencia

Pero regulación, ¿por parte de quién? Porque un aspecto importante es que las reglas difieren de un lugar a otro, tal y como planteó Jake Baker. Él vivía en Ann Arbor (Michigan), estaba sometido a sus leyes y, aparentemente, se adaptaba razonablemente bien a ellas. La autoridad de ese espacio gobernaba a Jake y cualquiera diría que le gobernaba totalmente.

En el ciberespacio, sin embargo, la conducta de Jake cambiaba, en parte porque las normas del espacio eran diferentes. Y eso desencadenó el problema. Y es que cuando Jake «iba al» ciberespacio, no abandonaba el espacio real, o más concretamente, no abandonaba Ann Arbor. Mientras permanecía sentado en su dormitorio de la Universidad de Michigan, era capaz de teletransportarse —en un sentido únicamente normativo— a un mundo diferente donde no gobernaban las normas de urbanidad y decencia que imperaban fuera de su habitación. El ciberespacio concedía a Jake la posibilidad de escapar de las normas de Ann Arbor y vivir conforme a las de otro lugar. Esto creó un conflicto de autoridades, dándole la posibilidad de seleccionar una u otra meramente mediante la conexión o desconexión de su ordenador.

Una vez más, no estoy planteando que en el espacio real no exista tal posibilidad —por supuesto que existe. Sin duda, hay un Jake que vive en Hackensack (una ciudad suburbana con valores suburbanos en el Estado de Nueva Jersey) y que conduce cada noche hasta el centro de Manhattan para vivir unas cuantas horas bajo las «reglas» del centro de Manhattan. Estas reglas no son las que imperan en Hackensack; la vida en Manhattan es diferente. Como el Jake de Ann Arbor, el Jake de Hackensack vive sometido a autoridades en conflicto; pero entre las vidas de ambos Jakes existe una diferencia de grado que deviene una diferencia cualitativa: el Jake de Ann Arbor plantea un problema más significativo para Ann Arbor que el que el Jake de Hackensack plantea para Hackensack. Las diferencias podrían ser mucho mayores y el efecto más intenso.

Tampoco deberíamos pensar de forma reduccionista acerca de las comunidades normativas en conflicto entre las que Jake podría moverse. «Escapar», en este sentido, podría ser tanto positivo como negativo: escapa el adolescente homosexual de una localidad pequeña cuando abandona sus normas mediante un *chat* homosexual de America Online,[25] y escapa también el pederasta que viola las normas de la sociedad ordinaria e induce a un niño a practicar sexo *online*.[26] Ambos tipos de escapada son posibilitados por la arquitectura del ciberespacio tal y como la conocemos hoy en día, pero nuestras actitudes hacia ellos son muy diferentes. Yo califico la primera de

---

25 Véase Steve Silberman, «We're Teen, We're Queer, and We've Got E-Mail», *Wired*, noviembre de 1994, pp. 76, 78 y 80, reeditado en Richard Holeton (ed.), *Composing Cyberspace: Identity, Community, and Knowledge in the Electronic Age*, Boston, McGraw-Hill, 1998, p. 116.

26 Cfr. *United States vs. Lamb*, 945 F.Supp 441 (NDNY 1996). (El propósito del Congreso al promulgar la *Child Protection Act* era regular la pornografía infantil a través de la transmisión informática, un interés legítimamente relacionado con el corte del flujo de pornografía infantil).

liberadora y la segunda de criminal; otros califican ambas de criminales; y otros califican ambas de liberadoras. Pero la cuestión no radica en nuestra forma de calificarlas, sino en las consecuencias de vivir en un mundo donde podemos habitar ambos tipos de espacio simultáneamente. Cuando 50 personas de 25 jurisdicciones de todo el mundo se pasan 2.000 horas construyendo una comunidad virtual en *Second Life* que está alojada en servidores de San Francisco, ¿qué reclamación deberían plantear las jurisdicciones del mundo real sobre esa actividad? ¿Cuál de las 25 jurisdicciones prevalece? ¿Qué soberanía debería imperar?

Estos cuatro temas constituyen el eje de lo que viene a continuación y, asimismo, cartografían el planteamiento que deseo reflejar en este libro. La regulación en el ciberespacio puede ayudarnos a comprender algo importante acerca de cómo funciona cualquier regulación y ésa es la lección del primer tema, «Regulabilidad». La regulación en el ciberespacio también introducirá un regulador («el código») cuya trascendencia aún no captamos plenamente, y en eso se centra el segundo tema, «Regulación mediante el código». Tal regulación tornará ambiguos ciertos principios que son fundamentales para nuestra tradición, de ahí que el tercer tema se llame «Ambigüedad latente». Dicha ambigüedad nos exigirá, en EEUU, tomar una decisión, pero esta decisión no será más que una entre las muchas que otros espacios soberanos habrán de tomar. En última instancia, lo más arduo será lidiar con estas «Soberanías en conflicto», cada una de las cuales tratará de marcar este espacio con sus propios valores distintivos.

Exploro estos cuatro temas en un contexto que, como dije al comienzo, ha cambiado significativamente desde la primera edición de esta obra. En el momento de escribirla, dos ideas parecían dominar el debate sobre la red: en primer lugar, que el Estado nunca podría regular la red; y, en segundo lugar, que eso era bueno. Hoy en día, estas actitudes han variado. Sigue vigente el lugar común de que el Estado no puede regular la red, pero, en un mundo inundado de correo basura, virus informáticos, robo de identidad, «piratería» y explotación sexual, la animadversión hacia la regulación ha declinado. Todos amamos la red, pero si algún estado pudiera realmente cumplir la promesa de eliminar todos los males de este espacio, la mayoría de nosotros lo firmaríamos encantados.

Ahora bien, por más que las actitudes hacia la red hayan evolucionado, mis opiniones no han cambiado. Sigo creyendo que la red puede ser regulada. Sigo creyendo que la consecuencia indiscutible de una serie de influencias obvias será un incremento radical de la capacidad estatal para regular esta red. Sigo creyendo también que, en principio, esto no

tiene por qué ser negativo. No estoy contra la regulación si está bien hecha. Creo que la regulación resulta esencial para preservar y defender ciertas libertades fundamentales.

Pero también creo que queda muy lejos el momento en que nuestro Estado en concreto pueda regular bien este contexto. Esto se debe tanto a un escepticismo general hacia nuestro Estado —basado en una aversión hacia la forma concreta de corrupción que define su funcionamiento— como a un escepticismo específico —porque aún no ha reconocido plenamente cómo funciona la regulación en la era digital.

Qué duda cabe que esta singular mezcla de visiones seguirá desconcertando a muchos. ¿Cómo puedo creer en la regulación y, sin embargo, mantener mi escepticismo hacia el Estado? Lo cierto es que no se necesita mucha imaginación para entender que estas visiones aparentemente conflictivas pueden ir de la mano. Asumo que todos creemos en el potencial de la Medicina, pero imaginémonos nuestra actitud si nos enfrentáramos con un «médico» que llevara un frasco de sanguijuelas. En mi opinión, habría mucho que hacer en este contexto, pero tenemos muy buenas razones para no desear hacer nada con este «médico» en concreto.

Primera parte

«Regulabilidad»

Se dice que el ciberespacio no puede ser regulado, pero, ¿qué significa decir que algo podría ser regulado? ¿Qué hace posible la regulación? La Primera Parte de esta obra aborda estas cuestiones. Si Internet no puede ser regulada, ¿por qué? Y, sea cual sea la razón, ¿puede cambiar tal situación? ¿Podría un espacio no regulable ser domesticado? ¿Podría derrotarse al Salvaje Oeste y cómo?

3. Es-ismo: ¿es como debe ser?

> El auge de un medio electrónico indiferente a los límites geográficos sume al Derecho en el desconcierto, al generar fenómenos completamente inéditos que han de someterse a normas legales claras, pero que ninguna forma de soberanía basada en la territorialidad puede gobernar de modo satisfactorio.
>
> David Johnson y David Post[1]

> Algunas cosas sobre el gobierno de la Red no cambian nunca. La más destacada es su capacidad innata para resistir casi cualquier forma de gobierno.
>
> Tom Steinert-Threlkeld[2]

SI HA HABIDO UN LUGAR COMÚN (o meme) al hablar del ciberespacio, ha sido el que proclamaba que éste era un lugar que no podía regularse; que el ciberespacio «no puede gobernarse», que su «naturaleza» se resiste a la regulación. No se dice que el ciberespacio no pueda romperse o que el Estado no pueda clausurarlo, sino que, a juicio de la primera generación de teóricos, el poder estatal sobre la conducta que se da allí es muy limitado. En esencia, el ciberespacio constituye un espacio sin control.

---

1 David R. Johnson y David Post, «Law and Borders—The Rise of Law in Cyberspace», *Stanford Law Review*, núm. 48, 1996, pp. 1367, 1375.

2 Tom Steinert-Threlkeld, «Of Governance and Technology», en *Inter@ctive WeekOnline*, 2 de octubre de 1998.

Naturaleza. Esencia. Innato. Las cosas son así. Este tipo de retórica debería suscitar sospechas en cualquier contexto, pero en éste de forma muy especial. Si existe un lugar donde no impera la «naturaleza», un lugar construido por la mano del hombre, ése es sin duda el ciberespacio. Sin embargo, la retórica «esencialista» encubre todo esto y desencamina nuestras intuiciones hacia rutas peligrosas.

He aquí la falacia del «es-ismo» —el error de confundir lo que algo es con lo que debe ser. Ciertamente el ciberespacio *es* de una determinada forma, pero no *ha de ser* necesariamente así. No existe una única forma o una única arquitectura que definan la naturaleza de la Red. Son muchas las posibles arquitecturas de lo que llamamos «la Red» y el carácter de la vida en el seno de cada una ellas es diverso.

Que la mayoría de nosotros incurra en esta falacia no es algo sorprendente. Y es que la mayoría de nosotros no tiene ni idea de cómo funcionan las redes, con lo cual difícilmente podría concebirlas de otra forma. Asumimos que las cosas son como deben ser. No estamos formados para contemplar todas las formas mediante las que la tecnología podría alcanzar los mismos fines con diferentes medios. Esa clase de formación es la que corresponde a los tecnólogos y la mayoría de nosotros no lo somos.

A lo largo de este libro, en cambio, subyace un único alegato normativo: que todos debemos aprender al menos lo suficiente como para captar que esta tecnología es moldeable, esto es, que puede modificarse para funcionar de formas diferentes. En este sentido, si los que sabemos muy poco sobre tecnología hemos de equivocarnos, que sea por imaginar la tecnología como moldeable por exceso y no por defecto. Deberíamos esperar —y reclamar— que la tecnología se construya como reflejo de un conjunto de principios que consideramos importantes; y que sobre los tecnólogos recaiga la obligación de mostrar por qué no puede ser atendida esa reclamación.

La particular confusión «es-ismo» que da título a este capítulo es aquélla que asevera que el ciberespacio no puede regularse. En este capítulo y en los que vienen a continuación, defiendo que tal idea es errónea. Que el ciberespacio sea o no regulable depende de su arquitectura. La arquitectura original de Internet dificultaba extremadamente la regulación. Ahora bien, dicha arquitectura original puede cambiar y, de hecho, sobran argumentos para afirmar categóricamente que *está cambiando*. Es más, estoy convencido de que bajo la arquitectura que emergerá, el ciberespacio será el espacio más regulable que jamás haya conocido el ser humano. Puede que una vez la «naturaleza» de la Red fuera la irregulabilidad, pero hoy esa «naturaleza» está a punto de transformarse por completo.

Para captar este giro, primero hemos de observar el contraste entre dos ciberlugares diferentes. Ambos constituyen dos tipos ideales, hasta tal punto que uno de ellos ya ha dejado de existir en la Red. Esto viene a confirmar el argumento que se trata de plantear en esta sección: que estamos pasando de una Internet a otra, que a su vez será significativamente más regulable.

Las descripciones que vienen a continuación no son técnicas. No las incluyo a modo de definiciones completas de tipos de redes o tipos de control, sino como ilustraciones, como bosquejos que nos permitan vislumbrar una idea mucho más general.

Ciberlugares: Harvard contra Chicago

Internet nació en las universidades estadounidenses y, por más que sus primeros usuarios fueran investigadores, la forma de vida que surgió con su nacimiento estaba ligada a la vida universitaria. Internet arrastró a multitud de estudiantes al mundo *online*, apartándolos de la vida en el espacio real. La Red fue uno de los muchos estupefacientes que circularon por los campus universitarios a mediados de los años noventa, y su importancia no ha dejado de crecer desde entonces. Como la ex columnista del *New York Times*, J. C. Herz, escribió en su primer libro sobre el ciberespacio:

> Cuando alzo la vista, veo en el reloj de pared que son las cuatro y media de la madrugada. «No puede ser». Consulto mi reloj de pulsera. Las cuatro y media. Llevo seis horas sin despegarme de la pantalla y parece como si no hubiera pasado el tiempo. No me encuentro ni remotamente cansada. Aturdida y sedienta, sí, pero nada cansada. Es más, estoy eufórica. Me apresuro a atiborrar mi mochila de un cúmulo caótico de manuales, artículos fotocopiados, rotuladores y notas, me precipito escaleras arriba como alma que lleva el diablo, paso junto al guardia de seguridad y salgo a la calle en medio de una neblina que anuncia el amanecer...
>
> Me detengo un segundo allí donde se juntan la acera húmeda y la seca. [...] Comienzo a pensar acerca de esta cosa que zumba por todo el mundo, a través de las líneas telefónicas, todo el día, toda la noche. Lo tenemos delante de nuestras narices y, sin embargo, es invisible. Es como

> *Narnia* o Magritte o *Star Trek*, todo un maldito mundo. Con la salvedad de que no existe físicamente. Es simplemente la conciencia colectiva de cuantas personas se encuentran en él.
>
> Realmente esto es algo extraordinariamente insólito.[3]

No todas las universidades, sin embargo, adoptaron la Red del mismo modo. Dicho de otra forma, el acceso a Internet que proporcionaban difería de unas a otras. Las normas eran distintas y también lo eran las libertades que se permitían. Un ejemplo de esta diferencia viene de dos instituciones que conocí bastante bien, pero habría otros muchos ejemplos igualmente ilustrativos.

A mediados de los noventa, si alguien quería acceder a Internet en la Universidad de Chicago, simplemente conectaba su máquina a las clavijas de ethernet situadas por toda la universidad.[4] Cualquier ordenador con conexión ethernet podía enchufarse en esas clavijas y, una vez conectado, disponía de pleno acceso a Internet —esto es, de acceso completo, anónimo y gratuito.

El motivo de esta libertad fue la decisión de un administrador —el por entonces rector Geoffrey Stone, antiguo decano de la Facultad de Derecho y destacado erudito en el ámbito de la libertad de expresión. Cuando la Universidad estaba diseñando su red, los técnicos consultaron a Stone si debía permitirse la comunicación anónima. Stone respondió afirmativamente, remitiéndose al principio de que las normas que regulan la libertad de expresión en la universidad debían protegerla tan celosamente como la Primera Enmienda; todo el mundo tendría derecho a comunicarse anónimamente en la Universidad, puesto que la Primera Enmienda a la Constitución garantiza el mismo derecho con respecto a los Estados. De esta decisión sobre la política universitaria emanó la arquitectura de la red de la Universidad de Chicago.

En Harvard, las normas eran diferentes. Si alguien enchufa su computadora a una entrada ethernet de la Facultad de Derecho de Harvard, no dispondrá de conexión a la Red. Nadie puede conectarse a la red en Harvard a

---

3 J. C. Herz, *Surfing on the Internet: A Nethead's Adventures On-Line*, Boston, Little Brown, 1995, pp. 2–3.

4 El diseño de la red de Chicago ha cambiado ligeramente desde que escribí estas páginas. Ahora se requiere cierto grado de autentificación pero, una vez que se asigna una dirección IP a los puertos ethernet, esa dirección se mantiene, «con tal de que no se produzcan malos comportamientos, no sabremos qué ha sucedido. En ese sentido, es en buena medida tal y como era». Grabación de audio: entrevista con Greg Jackson (1 de septiembre de 2006, incluida en el archivo del autor).

menos que su ordenador esté registrado —autorizado, aprobado, verificado— y sólo pueden registrar su ordenador los miembros de la comunidad universitaria. Una vez registrado, todas las interacciones en la red son vigiladas e identificadas con la máquina en cuestión. Además, para acceder a esta red universitaria, los usuarios han de «firmar» una especie de contrato que conlleva la aceptación de esta práctica invasiva de vigilancia. En esta red, no está permitida la expresión anónima —porque va contra las normas. Se puede controlar el acceso basándose en la identidad del usuario y se pueden rastrear las interacciones basándose en lo que dicho usuario realizó en la Red.

Este diseño emanó igualmente de la decisión de un administrador, en este caso de uno menos interesado en las protecciones de la Primera Enmienda. En Harvard, el ideal era el control, mientras que en Chicago fue el acceso; Harvard eligió tecnologías que posibilitaran el control; Chicago eligió aquéllas que facilitasen el acceso.

Estas dos redes se diferencian, al menos, en dos aspectos importantes. En primer lugar, es obvio que ambas redes difieren en los principios que abrazan.[5] Estamos, pues, ante una diferencia deliberada. En la Universidad de Chicago, los principios de la Primera Enmienda determinaban el diseño de la red; otros principios distintos regían el diseño de Harvard.

Pero estas redes también difieren en un segundo aspecto. Como en Harvard el acceso está controlado y se conoce la identidad del usuario, sus acciones pueden rastrearse hasta su punto de entrada en la Red. Como en Chicago el acceso no está controlado ni se conoce la identidad del usuario, sus acciones no pueden rastrearse. La vigilancia o el seguimiento de la conducta es más difícil en Chicago que en Harvard. De resultas, en la red de Harvard la conducta es más controlable que en la red de la Universidad de Chicago.

Ambas redes difieren, pues, en el punto hasta el cual hacen regulable la conducta en su seno. Esta diferencia es simplemente una cuestión de código —una diferencia en el software y el hardware que proporcionan acceso a los usuarios a la Red. Un código diferente determina una regulabilidad diferente de las redes. La regulabilidad se halla, por lo tanto, en función del diseño.

---

5 Véase Helen Nissenbaum, «Values in the Design of Computer Systems», *Computers and Society*, marzo de 1998, p. 38.

Estas dos redes constituyen simplemente dos puntos dentro de un espectro de posibles diseños de red. En un extremo del espectro se podría situar Internet —una red definida por un conjunto de protocolos abiertos y no propietarios, para cuyo acceso y uso no se requiere identificación personal alguna. En el otro extremo están las redes tradicionalmente cerradas, propietarias, que sólo permiten el acceso a quienes cuenten con autorización expresa; en ellas, en consecuencia, el control es muy estrecho. Entre estos extremos se hallan redes que mezclan elementos de ambas. Sobre la base de la irregulable Internet, estas redes mixtas agregan una capa de elementos de control superpuestos a la Red.

De esta forma, la red original de la Universidad de Chicago —que ha experimentado algunos cambios en los últimos años—[6] estaba muy cercana a la norma de acceso a la Internet de mediados de la década de los noventa,[7] a la que llamaremos Red´95. En el otro extremo están las redes cerradas que precedieron a Internet y aún existen hoy en día —por ejemplo, la red de cajeros automáticos, que permite sacar dinero de un banco de California a las dos de la madrugada desde Tblisi. Y, entre ambos extremos, hay redes como la de Harvard —redes que agregan una capa de control sobre el conjunto de protocolos que definen «Internet». Estos protocolos se denominan «TCP/IP» y los describo más ampliamente en el próximo capítulo. La característica

---

6 Como me describió el administrador de la red, Greg Jackson, por más que ciertos puertos (incluyendo los de la red *wireless*) requieran que el usuario registre inicialmente la máquina, no se realiza ningún esfuerzo destinado a verificar la identidad del usuario. Y, lo más importante, sigue habiendo un número importante de puertos que esencialmente permanecen sin regular. Esto no significa, no obstante, que el uso no esté regulado. Tal y como describió Jackson:

> Pero la verdad es que si llegamos a identificar una red P2P concreta con un tráfico enorme de películas, le asignaremos una prioridad inferior, de modo que simplemente vaya más lenta y no interfiera con el resto de gente. En este sentido, realizamos bastante catalogación de paquetes, pero casi nunca se llega a bloquear sitios concretos, por ejemplo; ha habido algún caso en que hemos tenido que hacerlo, simplemente porque...

Según Jackson, ahora es la Universidad de Columbia la que se ha ganado la reputación de disponer de la red más libre. «La Universidad de Columbia [...] en realidad no trata nunca de vigilar quién accede a la red local del campus, no se preocupa de eso. Su política es que la Universidad protege las aplicaciones, no la red en sí misma».

Grabación de audio: entrevista con Greg Jackson (1 de septiembre de 2006, incluida en el archivo del autor).

7 Para una descripción extremadamente legible al respecto, véase Peter Loshin, *TCP/IP Clearly Explained*, San Francisco, Morgan Kaufmann, 1997, pp. 15–23; véase también Craig Hunt, *TCP/IP Network Administration* (2ª), Sebastopol (Cal.), O'Reilly and Associates, 1998, pp. 8–22; Fred B. Schneider (ed.), *Trust in Cyberspace*, Washington (DC), National Academy Press, 1999, pp. 29–36.

esencial de la red de Harvard, en cualquier caso, es que ese conjunto de protocolos se vio complementado por elementos superpuestos, de modo que sólo se podía acceder a Internet tras haber superado esta capa de control.

Estos tres diseños se refieren a redes de comunicación que son «como» Internet. No obstante, sus diferencias suscitan una pregunta obvia: cuando se dice que Internet es «irregulable», ¿a qué red se está aludiendo? Y si se alude a una red irregulable, ¿por qué es irregulable? ¿Qué características de su diseño la hacen irregulable? Y, finalmente, ¿podrían ser diferentes dichas características?

Consideremos tres aspectos del diseño de la Red´95 que dificultan al regulador controlar la conducta en ella. Desde la perspectiva de un usuario amante del anonimato, se trata de «características» de la Red´95 —aspectos que hacen más valiosa esa red. Pero desde la perspectiva del regulador, tales características constituyen «errores» —imperfecciones que limitan la recopilación de información, ya sea sobre el usuario o sobre el material que está utilizando.

La primera de estas imperfecciones es la información sobre los usuarios —quién es la persona que está utilizando Internet. Como decían en una famosa viñeta (la del dibujante Peter Steiner en el *New Yorker*) dos perros sentados frente a un ordenador: «En Internet, nadie sabe que eres un perro».[8] Y nadie lo sabe porque los protocolos de Internet no exigen al usuario acreditar quién es antes de poder usarla. Insisto, los protocolos *de Internet* no exigen esa credencial; puede que sí lo haga nuestro punto de acceso local, como en el caso de la red de Harvard. Pero incluso en ese caso, la información que liga al individuo a una determinada operación por la red está en manos del proveedor de acceso, no es parte de su operación en Internet.

La segunda «imperfección» es la información sobre la geografía —dónde está la persona que está utilizando Internet. Como describiré en el capítulo 4, aunque Internet esté constituida por direcciones, éstas al principio no eran más que direcciones lógicas que no se correspondían con ninguna localización particular del mundo físico. En este sentido, cuando recibo un paquete de datos que me ha enviado el lector a través de Internet, ciertamente me resulta posible conocer la dirección de Internet desde la que llega el paquete, pero no la dirección física.

---

8 Peter Steiner, viñeta, *New Yorker,* 5 de julio de 1993, p. 61.

Y, finalmente, la tercera «imperfección» es la información sobre el uso —qué datos se envían a través de esta red y qué uso se hace de ellos. Internet no requiere ningún sistema concreto de etiquetado para enviar datos. De nuevo, como veremos en detalle más abajo, existen normas que dicen algo, pero ninguna regla que asegure que los datos se distribuyen de acuerdo con dichas normas. Nada coloca los bits en un contexto significativo, al menos no de un modo en que una máquina pudiera emplearlos. La Red´95 no exigía etiquetado alguno para los datos. Los «paquetes» de datos están etiquetados en el sentido de llevar una dirección, pero, más allá de eso, podrían contener absolutamente cualquier cosa.

Estas tres «imperfecciones» están enlazadas entre sí: puesto que no hay modo de saber quién es alguien, de dónde procede y qué está haciendo, tampoco hay modo de regular la conducta en la Red. Si no es posible descubrir quién hizo qué y dónde, no se pueden imponer fácilmente reglas que digan «prohibido hacer esto o, al menos, prohibido hacerlo ahí». O, expresado de otra forma, lo que no se puede saber determina qué se puede controlar.

Tomemos en consideración un ejemplo para clarificar esta idea. Pongamos que el Estado de Pensilvania desea bloquear el acceso de los niños a la pornogafía y, consecuentemente, promulga una ley que establece que «ningún niño de Pensilvania puede tener acceso a pornografía». Para hacer cumplir esa norma, el Estado de Pensilvania ha de averiguar (1) si alguien es o no un niño, (2) de dónde procede (de Pensilvania o del Estado de Maine), y (3) qué está buscando (pornografía o mazapán). Sin embargo, la Red´95 no le será de gran ayuda al Estado de Pensilvania para hacer cumplir esta norma. La gente que accede al contenido en Pensilvania mediante la Red´95 no tiene que revelar nada acerca de su identidad o su lugar de procedencia, y nada en el diseño de la Red´95 exige a los sitios la descripción del contenido que albergan. Estas lagunas informativas dificultan la regulación y, por consiguiente, el regulador las contempla como imperfecciones del diseño original de la Red.

Pero la red de Harvard sugiere que, como mínimo, es posible eliminar los «errores» de la Red´95. La Red podría conocer las credenciales del usuario (identidad y localización) y la naturaleza de los datos que se envían. Tal conocimiento podría incorporarse a la Red sin destruir su funcionalidad. En otras palabras, no se trata de elegir entre Internet o la ausencia de Internet, ni entre Internet y una red cerrada propietaria.

Harvard sugiere que existe una vía intermedia. Podrían superponerse a la Red una serie de arquitecturas de control para «corregir» y eliminar «imperfecciones»o, en otras palabras, para facilitar el control.[9]

He aquí el primer alegato, muy sucinto, de este capítulo inicial dentro de la historia sobre el control emergente: las arquitecturas de control son posibles y podrían añadirse a la Internet que hemos conocido, cambiando radicalmente su carácter. La decisión de si deberían o no ser añadidas depende de para qué deseemos usar dicha red.

Afirmo que se trata de un alegato sucinto porque, aunque lo considero importante, es una idea que parece obvia incluso si no se había pensado antes. Más que obvia, esta idea debería considerarse prosaica, pues la reconocemos en multitud de contextos. Pensemos, por ejemplo, en la oficina de Correos. Cuando yo era un crío, la oficina de Correos era un refugio de expresión anónima cuya función consistía simplemente en distribuir paquetes. Como la Red´95, esta oficina no se preocupaba de quién enviaba una carta o qué contenía un sobre o un paquete. Tampoco existía el requisito obligatorio de registrarse antes de enviar una carta, ni que la carta incluyera un remite que fuera correcto. Si se tenía cuidado de no dejar huellas dactilares, podía emplearse este servicio estatal para enviar mensajes perfectamente anónimos.

Obviamente, la oficina de Correos podría diseñarse de modo diferente. De este modo, el servicio podría exigir la inclusión de un remite en el envío, así como la verificación de que la dirección facilitada era correcta (por ejemplo, revisando el documento de identidad del remitente antes de aceptar un paquete). Podría incluso requerir una inspección antes de expedir un paquete o un sobre en concreto. Todos estos cambios en los procedimientos del servicio de correos producirían un mundo donde la correspondencia fuera muy fácil de vigilar y rastrear. Al diseñar así la oficina de Correos, el Estado está tomando esa opción. Si la vigilancia se vuelve relevante, el

---

9 En algunos contextos se denomina intranet a una arquitectura de red que resuelve algunas de estas «imperfecciones» —que inserta estos elementos de control. Estas redes internas son hoy en día la parte de Internet que más rápidamente crece, constituyendo un extraño híbrido de dos tradiciones en la informática de redes —los sistemas abiertos de Internet, basados en TCP/IP, y las redes propietarias tradicionales agregadas a Internet, basadas en una cierta capacidad el control. Las intranets combinan valores de ambas tradiciones para producir una red que es interoperativa pero que proporciona a sus propietarios un control sobre el acceso mayor del que podría darse en Internet. Mi tesis en este libro es que nuestra Internet se está transformando precisamente en una «internet» bajo control.

Estado puede cambiar el sistema para facilitarla; en caso negativo, puede dejar el sistema postal tal y como (en buena parte) está. Pero si el Estado cambia el sistema para posibilitar una vigilancia más sencilla, las modificaciones se reflejarán en los principios que informan el diseño de esa red.

En este libro defiendo que existen suficientes intereses para transformar la Red´95 de un espacio de anonimato por defecto, en otro de identificación por defecto. Por ahora, sin embargo, no he dicho nada que demuestre *cómo*. ¿Qué es lo que nos llevaría de la Red liberal relativamente irregulable a una Red de control altamente regulable?

Ésta es la pregunta clave de esta Primera Parte, que responderé en dos pasos sucesivos. En el Capítulo 4, defiendo que veremos la Red moverse hacia una arquitectura de control incluso sin la ayuda del Estado. En el Capítulo 5, esbozo de qué modo el Estado también podría contribuir. Las actuales tendencias nos traen la promesa de una Red altamente regulable — no la utopía de los liberales, ni tampoco la Red que nuestros padres (o, más probablemente, nuestros hijos) conocieron, sino una Red cuya característica esencial es su capacidad de control.

En otras palabras, una Internet que transforma lo que en otro tiempo fue Internet.

4. Arquitecturas de control

El Hombre Invisible no teme al Estado. Sabe que su naturaleza le coloca fuera su alcance (a menos que cometa alguna tontería, y, cómo no, siempre las comete). Su historia nos da la clave para una lección general: si no se puede saber quién es alguien, dónde está o qué está haciendo, no se le pueden aplicar las regulaciones. Ese alguien podrá hacer lo que le plazca y el Estado se verá impotente para impedírselo.

Eso mismo sucedía en la Internet original, ya que en ella todo el mundo era invisible. En sus orígenes, la arquitectura del ciberespacio ponía muy difícil averiguar quién era alguien, dónde estaba o qué estaba haciendo, con lo cual la regulación de las conductas resultaba igualmente complicada.

El objetivo del capítulo anterior era añadir una consideración pequeña, pero importante, a esta idea obvia: sea lo que sea el ciberespacio, no tiene por qué ser siempre así. La naturaleza de Internet no viene dada por Dios, sino que es producto de su diseño y éste podría ser diferente. La Red podría diseñarse para revelar quién es alguien, dónde está y qué está haciendo, en cuyo caso podría convertirse en el espacio más regulable que jamás se haya conocido, tal y como discutiré a lo largo de esta Primera Parte.

En este capítulo, describo los cambios que podrían —y, de hecho, lo están haciendo— convertir la Red de un espacio sin regulación a otro perfectamente regulado. Dichos cambios no los está diseñando el Estado, sino que son reclamados por los usuarios y desarrollados por el comercio. No son, pues, producto de ninguna conspiración inspirada en *1984*; son consecuencia de los cambios implementados con fines comerciales, puramente pragmáticos.

Obviamente, esto no determina la bondad o maldad de dichos cambios. Por ahora, mi intención no es normativa, sino meramente descriptiva. Deberíamos comprender hacia dónde vamos y por qué, antes de preguntarnos si eso es o no lo que queremos.

La historia del futuro de Internet fue escrita en Alemania en enero de 1995. La legislación alemana regulaba la pornografía, en el Estado de Baviera dicha legislación era especialmente dura. El proveedor estadounidense de Internet CompuServe puso pornografía a disposición de sus usuarios (en buena medida, a través de USENET), entre ellos los ciudadanos de Baviera. Ante esto, el gobierno bávaro amenazó a los ejecutivos de CompuServe con sancionarlos si no eliminaban de sus servidores los contenidos pornográficos.

Al principio, CompuServe objetó que no podía hacer nada al respecto — excepto eliminar la pornografía de todos sus servidores, repartidos por todo el mundo. Eso a los alemanes no les preocupó demasiado, pero a CompuServe sí. De este modo, en enero de 1995, la compañía anunció una solución técnica: en lugar de bloquear el acceso a los grupos de USENET denunciados desde Baviera para todos sus usuarios, CompuServe ideó una tecnología que permitía filtrar el contenido por países.[1]

Para que tal solución funcionase, CompuServe tenía que empezar a indagar quién era cada usuario, qué estaba haciendo y dónde, para lo cual podía servirse de la tecnología. A partir de esta modificación, el futuro estaba marcado. En adelante, ante cualquier problema de regulabilidad, se replicará con esta respuesta obvia.

CompuServe no es Internet, por supuesto, pero su reacción sugiere el patrón que seguirá ésta. En este capítulo, esbozaré cómo Internet puede modificarse para funcionar (al menos en este aspecto) como CompuServe.

¿*Quién* hizo qué y dónde?

Para regular, el Estado necesita encontrar un modo de averiguar el «quién» de la pregunta «¿quién hizo qué y dónde?». Para entender cómo la Red puede dar esta información al Estado, hemos de examinar algo más acerca del funcionamiento general de la «identificación» y de cómo podría funcionar en Internet.

---

1 TelecomWorldWire, «Compuserve Moves for Porn Techno Fix», 11 de enero de 1995.

Identidad y autentificación: el espacio real

Para entender las tecnologías que se usan para identificar quién es alguien, consideremos la relación entre tres ideas familiares: (1) «identidad», (2) «autentificación» y (3) «credencial».

Para mí, la «identidad» implica algo más que quién es alguien, abarca también sus «atributos» o, más ampliamente, todos los hechos ciertos acerca de una persona (o de una empresa o de un objeto). En este sentido, la identidad de ese alguien incluye su nombre, su sexo, su lugar de residencia, su nivel educativo, el número de su carné de conducir, el de la Seguridad Social, sus compras en Amazon.com, si es abogado de profesión, etc.

Las demás personas conocen estos atributos al serles comunicados. En el espacio real, algunos atributos se comunican-perciben automáticamente: el sexo, el color de piel, la altura, la edad, o una sonrisa bonita, por ejemplo. Otros no se pueden conocer a menos que los revele la propia persona o alguien que la conozca: la nota media de Bachillerato, el color preferido, el número de la Seguridad Social, la última compra en Amazon, la admisión en el Colegio de Abogados.

Ahora bien, no basta con revelar un atributo para que la gente se lo crea («¡¿De verdad te han admitido en el Colegio de Abogados?!»), sino que, a menudo, la credibilidad dependerá de un proceso de «autentificación». En general, recurrimos a este proceso cuando queremos cerciorarnos de la veracidad de una determinada afirmación, más allá de la confianza que nos inspire quien la pronuncia. «Estoy casado», dice él. «Enséñame tu anillo», replica ella.

La primera de estas declaraciones es la afirmación de un atributo que el hombre alega tener; la segunda es una demanda de autentificación. Podríamos imaginar cómo se prolongaría dicha demanda (al menos en una comedia): «Oh, venga ya, eso no es un anillo de boda. Enséñame tu certificado de matrimonio». En un momento determinado, la demanda cesa, bien porque ya se han obtenido suficientes garantías, bien porque los requerimientos se han hecho demasiado extravagantes.

A veces, este proceso de autentificación es relativamente automático, ya que ciertos atributos son relativamente auto-autentificables: alguien afirma ser una mujer y puedo comprobarlo con sólo verla; alguien afirma ser un hablante nativo y lo puedo acreditar en cuanto hable con él. En ambos casos,

por supuesto, me podrían engañar, por lo que si mi vida dependiera de ello, puede que tomara otras medidas para cerciorarme de aquello que parece claro en apariencia. Ahora bien, en la mayoría de las situaciones, cuando se trata de los atributos más familiares, aprendemos a evaluarlos tan sólo con nuestro juicio individual.

Otros atributos, en cambio, no pueden autentificarse por sí mismos. Alguien dice que posee el título para pilotar un avión y yo quiero que me lo enseñe. Alguien dice que pertenece al Colegio de Abogados de California y yo quiero ver su licencia. Alguien dice que está cualificado para realizarle a mi padre una operación a corazón abierto, y yo quiero ver pruebas que me hagan confiar en que eso es cierto. De nuevo, estas «cosas» autentificadoras podrían falsificarse y mi confianza sería injustificada, pero si cuido de que el proceso de acreditación se corresponda al nivel de confianza que necesito, estoy actuando de modo bastante racional. Y la mayoría solemos apañárnoslas sin procesos de autentificación tremendamente complicados.

Una herramienta importante que a veces se emplea en este proceso de autentificación es la credencial. Entiendo por «credencial» un dispositivo normalizado para autentificar (hasta cierto nivel de confianza) una afirmación realizada. En este sentido, un carné de conducir es una credencial que certifica la condición de conductor. Generalmente estamos familiarizados con la forma de dichos carnés, de modo que confiamos en que seremos capaces de determinar si un carné concreto es válido o no. En ese mismo sentido, un pasaporte también es una credencial. Su finalidad es establecer la ciudadanía de la persona, identificándola mediante atributos relativamente auto-autentificables. Una vez más, estamos familiarizados con la forma de esta credencial y esto nos proporciona un nivel relativamente alto de confianza acerca de los datos contenidos en el pasaporte.

Obviamente, algunas credenciales son mejores que otras; algunas están construidas para dar más confianza que otras; algunas son más eficaces en proporcionar dicha confianza que otras. Pero, de entre todas las credenciales disponibles, elegimos aquéllas que se ajusten al nivel de confianza que necesitamos.

Pongamos un ejemplo obvio para reunir todas estas consideraciones: imagínese usted, el lector, que es cajero de un banco. Alguien aparece ante usted y declara que es titular de la cuenta # 654–543231, solicitando retirar todo el dinero.

En el sentido que he descrito, ese alguien (llamémosla Señora X) ha afirmado un hecho acerca de su identidad —que es la titular de la cuenta # 654–543231. Ahora es su tarea verificar tal afirmación, así que busca en el ordenador los registros de la cuenta en cuestión y descubre que hay un montón de dinero en ella. Ante esto, el deseo del lector de realizar una autentificación fiable es más acuciante si cabe. Le pregunta a la Señora X su nombre y el nombre que da coincide con el que figura en la cuenta. El lector gana cierta confianza y, a continuación, le pide a la Señora X dos formas de identificación, las cuales coinciden con ella. Su confianza aumenta cada vez más. Le pide a la Señora X que firme un resguardo de extracto de cuenta y la firma parece coincidir, con lo que el lector gana más confianza. Finalmente, el lector se fija en que la cuenta fue abierta por su directora, con lo que acude a preguntarle si reconoce a la mujer que está en el mostrador como la Señora X y la directora lo confirma. Ahora usted tiene suficiente confianza para entregarle todo el dinero de la cuenta # 654–543231.

Nótese que, a lo largo de este proceso, se han empleado tecnologías que ayudan a verificar que el atributo afirmado por la Señora X es cierto. El ordenador del banco relaciona un nombre con un número de cuenta; el carné de conducir o el pasaporte liga una fotografía a un nombre; y el ordenador guarda una copia de la firma. Todas éstas son tecnologías para incrementar la confianza.

Y nótese también que podríamos imaginar tecnologías aún mejores para incrementar dicha confianza. Las tarjetas de crédito, por ejemplo, se desarrollaron en una época en que su mera posesión autentificaba su uso. Tal diseño crea incentivos para robar tarjetas de crédito. Las tarjetas de cajero automático son diferentes —junto a su posesión, estas tarjetas requieren introducir una contraseña. Tal diseño reduce el valor de las tarjetas robadas. Pero hay quien escribe la contraseña en la propia tarjeta, o la lleva apuntada en la cartera junto a su tarjeta. Esto implica que el riesgo de robo no se elimina totalmente, si bien tal riesgo podría reducirse aún más mediante otras tecnologías de autentificación. Así, por ejemplo, ciertas tecnologías biométricas, como los lectores de huellas dactilares o los escáneres oculares, incrementarían la confianza en que el portador de una tarjeta está autorizado a usarla. (Aunque estas tecnologías a su vez pueden generar sus propios riesgos: en una conferencia oí a un vendedor describir una nueva tecnología para identificar a alguien a partir de la huella de su mano; un asistente preguntó si la mano tenía que estar *viva* para que funcionara la autentificación. El vendedor se quedó completamente pálido y, un momento después, respondió: «Supongo que no»).

En la vida real, estamos negociando constantemente estos procesos de autentificación, que pueden realizarse a mayor distancia cuanto mejores sean las tecnologías y las credenciales de las que dispongamos. En una ciudad pequeña, en una época más tranquila, las credenciales resultaban innecesarias. Se nos conocía por nuestro rostro, el cual acarreaba consigo una referencia (inscrita en el conocimiento común de la comunidad) acerca de nuestro carácter. Pero a medida que la vida se hace más móvil, las instituciones sociales dependen de otras tecnologías para construir confianza acerca de importantes afirmaciones sobre la identidad. Las credenciales se convierten, así, en una herramienta indispensable para asegurar tal autentificación. Si las tecnologías de autentificación pueden ser mejores o peores, entonces, obviamente, muchos tendrán interés en que sean mejores. Todos estaríamos mejor si pudiéramos validar ciertos hechos acerca de nosotros mismos de forma más fácil y fiable. El comercio también estaría sin duda mejor con mejores tecnologías de autentificación. Las tecnologías defectuosas generan fraude y el fraude es un coste improductivo para los negocios, de modo que si se pudiera eliminar mediante tecnologías mejores, los precios podrían bajar y podrían crecer los beneficios.

Y, finalmente, los Estados se benefician de mejores tecnologías de autentificación. Si verificar la edad fuera sencillo, entonces se podrían hacer cumplir las leyes que se aplican en función de la edad (relativas al consumo de alcohol o de cigarrillos). Y si fuera sencillo autentificar la identidad, entonces el Estado podría averiguar más fácilmente quién hizo qué.

Fundamentalmente, la regulabilidad de la vida en el espacio real depende de ciertas arquitecturas de autentificación. El hecho de que unos testigos puedan identificar a la persona que cometió un crimen, ya sea porque la conocen o por rasgos auto-autentificables como «era un varón blanco de metro ochenta de estatura», aumenta la capacidad estatal para perseguir dicho crimen. Si los criminales fueran invisibles o los testigos carecieran de memoria, se incrementarían los crímenes. El hecho de que las huellas dactilares sean difíciles de cambiar y de que ahora se cotejen automáticamente con el registro de criminales convictos eleva la posibilidad de atraparlos de nuevo. Si la policía se basara en una característica física más alterable, se reduciría su capacidad de seguir la pista a los reincidentes. El hecho de que los coches lleven matrículas y estén registrados a nombre de su dueño eleva la posibilidad de atrapar a un conductor que se da a la fuga tras un atropello. Sin matrículas ni sistemas de registro de propietarios, sería extremadamente difícil perseguir los crímenes automovilísticos. En todos estos casos, y en muchos otros, las tecnologías de autentificación del espacio real hacen posible regular la vida en él.

Estos tres intereses separados apuntan, pues, a un interés común; pero esto no implica afirmar que toda tecnología de autentificación responde a ese interés común, ni que estos intereses serán suficientes para facilitar una autentificación más eficaz. Lo que implica es que podemos ver hacia dónde empujan dichos intereses. Una mejor autentificación puede beneficiar a todos.

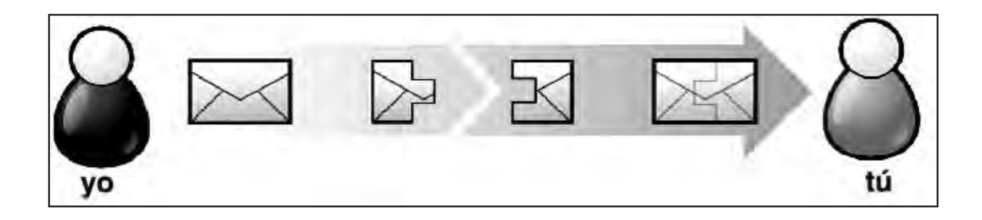
Identidad y autentificación: ciberespacio

En teoría, la identidad y la autentificación son idénticas en el espacio real y en el ciberespacio, pero en la práctica difieren bastante. Para captar esta diferencia, hemos de analizar algo más los detalles técnicos de la construcción de la Red.

Como ya he dicho, Internet está construida a partir de un conjunto de protocolos denominado «TCP/IP», que incluye en su núcleo protocolos de intercambio de paquetes de datos entre dos máquinas «a través» de la Red.[2] Dicho de un modo brutalmente simplificado, el sistema coge un puñado de datos (un archivo, por ejemplo), lo trocea en paquetes y marca sobre ellos la dirección y el remite correspondientes. Las direcciones se llaman direcciones IP (de *Internet Protocol*) y son algo así: 128.34.35.204. Una vez adecuadamente marcados, los paquetes se envían a través de Internet a su destino previsto. Por el camino, unas máquinas (los *routers*) miran la dirección a la que se envía el paquete, y, dependiendo de un algoritmo (cada vez más complicado), deciden a qué máquina enviar el paquete a continuación. Hasta llegar a su destino, un paquete puede dar muchos «saltos», pero, a medida que la red se hace más fuerte y robusta, dichos saltos parecen casi instantáneos.

---

2 Véase Ed Krol, *The Whole Internet: User's Guide and Catalogue*, Sebastopol (Cal.), O'Reilly and Associates, 1992, pp. 23–25; Loshin, *TCP/IP Clearly Explained*, op. cit., pp. 3–83; Hunt, TCP/IP, *op. cit.*, pp. 1–22; véase también Ben M. Segal, «A Short History of Internet Protocols at CERN», disponible en http://ben.home.cern.ch/ben/TCPHIST.html.



En los términos que he descrito, hay muchos atributos que podrían asociarse con un paquete de datos enviado a través de la Red. Por ejemplo, el paquete podría provenir de un correo electrónico escrito por Al Gore, lo que significa que lo ha enviado un ex vicepresidente de EEUU, un erudito acerca del cambio climático, un señor alto de más de 50 años, un ciudadano estadounidense, un ex senador de EEUU, etc. Imaginémonos también que el correo electrónico fue escrito mientras Al Gore estaba en Alemania y que trataba sobre las negociaciones para controlar el cambio climático. Podría decirse que la identidad de ese paquete de datos incluye todos estos atributos.

Ahora bien, el correo electrónico no autentifica por sí mismo ni uno solo de estos hechos. En el correo puede figurar que proviene de Al Gore, pero el protocolo TCP/IP por sí solo no nos da ninguna seguridad al respecto; puede que dicho correo haya sido escrito mientras Al Gore estaba en Alemania, pero podría haber sido enviado a través de un servidor situado en Washington; y, por supuesto, por más que el sistema se percate de que el paquete forma parte de un correo electrónico, la información que se transmite a través del protocolo TCP/IP no contiene en sí misma nada que indique de qué trata el mensaje. Así pues, el protocolo no autentifica a quién envió el paquete, desde dónde lo envió y cuál es su contenido, sino que sólo permite certificar a qué dirección IP se envió y desde qué dirección IP fue enviado. Desde la perspectiva de la red de transmisión, el resto de información es un excedente innecesario. Como un trabajador de Correos cuya mente vuela mientras trabaja, dicha red se limita a mover los datos y deja su interpretación en manos de las aplicaciones situadas a uno y otro extremo de la cadena de transmisión.

Tal minimalismo en el diseño de Internet no fue producto de un accidente, sino que refleja una decisión sobre cómo diseñar mejor una red de transmisión que realice eficazmente una amplia gama de funciones. En vez de construir en esta red un conjunto complejo de funcionalidades que pudiera necesitar cada aplicación concreta, su diseño traslada la complejidad a los extremos de la red —a las aplicaciones que se conectan a ella, más que a su

propio núcleo. Dicho núcleo se mantiene tan simple como sea posible. Por lo tanto, si es necesario autentificar quién es alguien o cifrar el contenido, tales funciones deberían incorporarse mediante una aplicación conectada a la red, no a través de la propia red.

Este principio de diseño fue denominado por los arquitectos de redes Jerome Saltzer, David Clark y David Reed el «principio de conectividad punto a punto»,[3] y ha sido un pilar fundamental de la arquitectura de Internet. En mi opinión, tal principio constituye una de las razones más importantes por las que Internet ha disfrutado de tal grado de innovación y desarrollo. Ahora bien, con los protocolos básicos de Internet por sí solos, resulta extremadamente difícil la identificación y la autentificación. En este sentido, es como si nos encontráramos en medio de una fiesta de carnaval, en penumbra y con voces llegándonos de todas partes, provenientes de gente que no conocemos y de lugares que no podemos identificar. El sistema capta que hay entidades externas interactuando con él, pero no sabe nada acerca de ellas. Mientras que en el espacio real —y ésta es la cuestión fundamental— el anonimato ha de crearse, en el ciberespacio el anonimato viene dado por defecto.

Identidad y autentificación: regulabilidad

Esta diferencia arquitectónica entre el espacio real y el ciberespacio marca a su vez una gran diferencia en la regulación de la conducta en cada uno de ellos. La ausencia de hechos relativamente auto-autentificables en el ciberespacio hace extremadamente difícil regular la conducta en él. Si en el espacio real pudiéramos ir por ahí como «El Hombre Invisible», podría decirse lo mismo. El hecho de que no podamos volvernos invisibles en el espacio real (o, al menos, no de forma sencilla) es un motivo importante por el que la regulación puede funcionar.

Así, por ejemplo, si un Estado quiere controlar el acceso infantil al lenguaje «indecente» en Internet, la arquitectura original de la Red le será de escasa ayuda. El Estado puede requerir a los sitios web: «No dejen que los

[3] Véase Jerome H. Saltzer et al., «End-to-End Arguments in System Design», en Amit Bhargava (ed.), *Integrated Broadband Networks*, Norwood (Mass.), Artech House, 1991, pp. 30–41.

niños vean porno». Ahora bien, los operadores de los sitios no tienen manera de saber —al menos con la información que proporciona el protocolo TCP/IP— si la entidad que entra en su página es un niño o un adulto. He aquí otra diferencia con el espacio real, donde un niño está abocado al fracaso si trata de entrar en una tienda pornográfica camuflado con un bigote postizo y encaramado en unos zancos. El atributo «ser un niño» se manifiesta en el espacio real, por más que puedan realizarse esfuerzos para disimularlo. Pero en el ciberespacio, no hace falta disimulo alguno, pues aquello que se pueda querer disimular acerca de la identidad (por ejemplo, que se es un niño) no se manifiesta de ninguna forma.

Todo lo anterior es cierto, al menos sobre la base de la arquitectura básica de Internet; los diez últimos años han evidenciado que no es así por necesidad. En la medida en que la falta de tecnologías de autentificación eficaces dificulta la regulación de la conducta, existen capas de arquitectura que podrían agregarse al protocolo TCP/IP para favorecer una autentificación eficaz. Estamos ya suficientemente inmersos en la historia de Internet para examinar cómo podrían configurarse estas tecnologías, y también para constatar que la tendencia hacia la autentificación es imparable. La única cuestión es si incluiremos en este sistema de autentificación los tipos de protección de la privacidad y de la autonomía que son necesarios.

Arquitecturas de identificación

La mayoría de usuarios de Internet no tiene ninguna conciencia de si su conducta está siendo vigilada o de si puede ser rastreada. Más bien al contrario, la experiencia de la Red nos sugiere anonimato. La Wikipedia no me recibe con un «Bienvenido de nuevo, Larry» cuando me conecto a su sitio para consultar una entrada, ni tampoco Google. Supongo que la mayoría de internautas interpreta esta falta de reconocimiento como una muestra de que nadie se percata de su presencia.

No obstante, las apariencias engañan. De hecho, a medida que Internet fue madurando, las tecnologías que vinculan conducta e identidad experimentaron un drástico incremento. Aún podemos tomar medidas que aseguren el anonimato en la Red, por supuesto, y muchos dependen de esto para hacer cosas buenas (como los defensores de los derechos humanos de Birmania) o

malas (coordinar planes terroristas). Pero conseguir ese anonimato requiere esfuerzo. El uso que la mayoría de nosotros hace de Internet se ha vuelto rastreable en un grado que jamás habríamos creído ni tan siquiera posible.

Consideremos en primer lugar la rastreabilidad resultante de los protocolos básicos de Internet —el conjunto de protocolos TCP/IP. Cuando efectuamos una petición para acceder a una página web, el servidor web necesita saber adónde enviar los paquetes de datos que aparecerán como una página web en nuestro navegador. Así pues, nuestro ordenador le indica al servidor dónde nos encontramos —al menos le indica un espacio IP— revelándole una dirección IP.

Como ya he descrito, la dirección IP en sí misma no revela nada acerca de quién es alguien, o de qué espacio físico procede, pero sí que permite un cierto grado de rastreo. Si (1) hemos accedido a la Red a través de un proveedor de servicios de Internet (PSI) que nos asigna una dirección IP mientras estamos conectados, y (2) ese PSI conserva los registros de dicha asignación, entonces es perfectamente posible que rastree nuestra navegación hasta llegar a nosotros.

¿Cómo?

Bien, imagínese el lector que está enojado con su jefa, a la que considera una fanfarrona que está llevando la empresa a la bancarrota. Tras meses de frustración, el lector decide hacer público su enojo. No «público» en el sentido de convocar una rueda de prensa, sino de escribir en un foro de Internet donde se discute acerca de su empresa.

El lector sabe que se metería en un buen lío si se le pudiera relacionar con las críticas que vierta en el foro, así que toma medidas para garantizar su «anonimato». Así, opta por abrir una cuenta en el foro con un nombre ficticio, con el cual el lector se siente seguro. Puede que su jefa lea sus comentarios desabridos, pero incluso si consiguiera que el anfitrión del foro le revelara los datos que el lector introdujo al inscribirse, daría igual porque todos son falsos. Su secreto, cree el lector, está a salvo.

Se equivoca. Además de la identificación que su nombre de usuario podría proporcionar, si el foro está en la web, se puede localizar la dirección IP desde la que el lector escribió sus comentarios. Con esa dirección IP y la hora a la que entró en el foro, es simple identificar el PSI que dio acceso a Internet por medio de «una búsqueda DNS inversa» (por las siglas en inglés

de *Domain Name System*).[4] Y, cada vez más, al PSI le resulta relativamente simple comprobar sus registros para revelar qué cuenta estaba usando esa dirección IP a la hora especificada. Por lo tanto, el PSI podría (si así se le requiriera) señalar la cuenta del lector como la que estaba utilizando la dirección IP desde la que se escribió el mensaje desabrido dirigido a la jefa. El lector puede intentar negarlo si quiere («¡Eh, en Internet nadie sabe que eres un perro!»), pero yo le recomendaría desistir cuanto antes. Ha sido atrapado por la Red. A perro flaco, todo son pulgas.

Una vez más, ¿qué hizo posible este rastreo? No fue ningún plan de la NSA (Agencia Nacional de Seguridad) ni ninguna estrategia de Microsoft. Lo que hizo posible el rastreo fue más bien una consecuencia de la arquitectura de la Red y de la arquitectura del acceso de pago a la Red de los PSI. La página web necesita conocer la dirección IP; los PSI requieren identificación para asignar una dirección IP a un cliente. Con tal de que se conserven los registros del PSI, la operación será rastreable. Moraleja: quien quiera anonimato, ¡que use un cibercafé!

Esta rastreabilidad en Internet suscitó una importante inquietud a comienzos del año 2006. Google anunció que rehusaría el requerimiento gubernamental de proporcionar los registros de un millón de búsquedas realizadas por sus usuarios en una semana. (Tanto MSN como Yahoo! habían accedido ya a la misma demanda). Tal requerimiento formaba parte de una investigación gubernamental que pretendía respaldar su defensa de un reglamento diseñado para bloquear el acceso infantil a la pornografía. Por más que el requerimiento prometiera que la información se usaría exclusivamente con dicho propósito, la comunidad de Internet se mostró profundamente preocupada ante estos hechos. Dependiendo de los datos que conservara Google, el requerimiento en principio demostraba que era posible rastrear búsquedas legalmente controvertidas hasta dar con direcciones IP individuales (y, de ahí, con individuos con cuenta en Google). Así, por ejemplo, si la dirección de Internet del lector en su trabajo es una dirección IP fija, entonces es posible que todas y cada una de las búsquedas que haya hecho desde el trabajo hayan quedado registradas en la base de datos de Google. ¿Le inquieta eso? Asuma el lector por el momento que no es un terrorista: ¿seguiría inquietándole eso?

---

4 Shawn C. Helms, «Translating Privacy Values with Technology», *Boston University Journal of Science and Technology Law*, núm. 7, 2001, pp. 288, 296.

Un vínculo a una dirección IP, sin embargo, sólo facilita el rastreo y, de nuevo, incluso en ese caso se trata de una rastreabilidad imperfecta. Los PSI no conservan los datos mucho tiempo (normalmente); algunos incluso no llevan ningún registro de asignación. Y si hemos accedido a Internet desde un cibercafé, entonces no hay razón para creer que la navegación puede ser rastreada. Por lo tanto, Internet sigue procurándonos todavía un mínimo de anonimato.

Ahora bien, el rastreo IP no es la única capa de arquitectura de identificación que se ha agregado a Internet. Al comienzo de la historia de la Web, se desarrolló una tecnología mucho más invasiva para aumentar su valor de cara al comercio y a sus clientes. Se trata de las denominadas *cookies*.

Cuando se lanzó la *World Wide Web*, el protocolo sólo permitía ver contenido que hubiera sido marcado en un lenguaje especial de programación. Este lenguaje (HTML) facilitaba los enlaces a otras páginas y simplificaba la aplicación de un formato básico al contenido (introduciendo negritas o cursivas, por ejemplo). Ahora bien, dicho protocolo no permitía que un sitio web pudiera saber fácilmente qué máquinas habían accedido a él. Se trataba de un protocolo «sin estado», que no guardaba información sobre conexiones anteriores. Y es que cuando un servidor web recibía una petición de acceso a una página, no conocía nada acerca del estado previo de la máquina, al no guardar información sobre conexiones anteriores.[5]

Desde la perspectiva de la privacidad, esto parece una característica genial de la Web. ¿Por qué tendría un sitio web que saber algo de mí si accedo a él en busca de algún contenido? No hay que ser un criminal para apreciar el valor de la navegación anónima. Imagínese el lector que las bibliotecas mantuvieran registros de cada vez que alguien abre un libro, aunque sólo sea por un segundo.

Desde la perspectiva del comercio, en cambio, esta «característica» de la Web original no es más que un fallo, y no porque los sitios comerciales necesariamente quieran saber todo de nosotros. Se trata más bien de un problema mucho más pragmático. Digamos que el lector va a Amazon.com e indica que desea comprar 20 ejemplares de mi último libro. (Inténtelo. Es divertido). Ahora su «carro de la compra» tiene 20 ejemplares de mi libro. A continuación, el lector pulsa sobre el icono de verificación de compra y se percata de

---

5 Para una descripción de los protocolos HTTP tal y como se empleaban a principios de los noventa, véase http://www.w3.org/Protocols/HTTP/HTTP2.html.

que su carro de la compra está vacío. ¿Por qué? Simplemente porque la Web, en su arquitectura original, no tenía modo de reconocer que el lector era la misma entidad que acababa de reservar 20 libros. Dicho de otro modo, el servidor *pasaba página*: la construcción original de la Web impedía que se recordara el paso de una página a otra. De resultas, la Web no era de mucha utilidad para el comercio.

Pero, como he repetido hasta la saciedad, el diseño original de la Web no tenía por qué ser así necesariamente. Y he aquí que los desarrolladores de la infraestructura de la Web comenzaron rápidamente a discurrir cómo podría «mejorarse» la Web para facilitar el comercio. Las *cookies* fueron la solución. En 1994, Netscape introdujo un protocolo para permitir que un servidor depositara un pequeño fragmento de información en aquellos ordenadores que accedieran a él. Este pequeño fragmento de información —la *cookie*— posibilitaba que el servidor reconociera los ordenadores en cuestión cuando accedían a otra página. Por supuesto, existen otros muchos recelos acerca de lo que podría llegar a posibilitar esa *cookie*, de los cuales nos ocuparemos en el capítulo dedicado a la privacidad. Por ahora, sin embargo, la cuestión fundamental no es los peligros que esta tecnología engendra, sino cuál es su potencial y cómo se construyó. Un pequeño cambio en el protocolo de interacción cliente-servidor permite ahora a los sitios web vigilar y seguir la pista a sus usuarios.

Sin duda, estamos ante un pequeño paso hacia la autentificación de identidad, por más que ésta aún quede lejos. Nosotros no somos nuestro ordenador (todavía), pero las *cookies* posibilitan que el ordenador autentifique que se trata de la misma máquina que accedió a un sitio web hace un momento. Y es sobre la base de esta tecnología como se construyó inicialmente todo el comercio electrónico. En adelante, los servidores serían capaces de «reconocer» que una determinada máquina es la misma que ya se conectó previamente, lo cual pondría en sus manos un gran tesoro.

Conviene recalcar una vez más que, en sentido estricto, las *cookies* no son más que una tecnología que simplifica el proceso de rastreo de la navegación que una máquina realiza a través de diferentes páginas web. Tal rastreo no necesariamente revela información acerca del usuario. Del mismo modo que en el espacio real podríamos seguir un rastro de migajas de galleta que nos llevara a una habitación vacía, un servidor web podría seguir un rastro de «clics de ratón» desde el primer acceso al sitio hasta que el usuario se desconecta de él. En ambos casos, nada se revela necesariamente acerca del usuario.

Ahora bien, a veces sí que se revela algo importante acerca del usuario mediante la asociación de esos datos con los recopilados por otra vía. Por ejemplo, imagínese el lector que entra en un sitio que le solicita que revele su nombre, su número de teléfono y su dirección de correo electrónico como condición para participar en un concurso. El lector confía en el sitio web y le da esos datos, abandonándolo a continuación. Al día siguiente, el lector vuelve a entrar en el sitio y consulta algunas de sus páginas. En esta interacción, por supuesto, no se revela nada. Pero si el servidor depositó a través del navegador una *cookie* en el ordenador del lector (y éste no ha tomado medidas para eliminarla), cuando el lector vuelva al sitio web, este le «reconocerá» y asociará todos aquellos datos con él. La *cookie* rastrea el ordenador del lector, y tal rastreo remite a un lugar en el que éste proporcionó información que la máquina no podría conocer de otra forma.

Tanto la rastreabilidad de las direcciones IP como las *cookies* se dan ahora por defecto en Internet. Qué duda cabe que hay formas de eludir esa rastreabilidad, pero la inmensa mayoría de nosotros no las aplicamos. Afortunadamente, para la sociedad y para la mayoría de nosotros, lo que hacemos en la Red no le importa realmente a nadie. Ahora bien, en el caso de que *sí* que le importase a alguien, no le resultaría muy complicado dar con nuestro paradero. Somos gente que va dejando migajas de «clics de ratón» a cada paso que da.

Esta rastreabilidad por defecto, sin embargo, no es suficiente para algunos, que reclaman algo más. Ésa era la postura de Harvard, como apunté en el capítulo anterior; y ésa es la postura que comparten casi todas las redes privadas hoy en día. Se ha desarrollado una variedad de tecnologías que posibilita una autentificación más estricta de los usuarios de la Red. En esta sección, describiré dos de estas tecnologías, si bien la segunda de ellas, a mi entender, demostrará ser la más importante.

La primera es la tecnología de *Single Sign-on* (SSO). Esta tecnología permite que alguien se identifique una sola vez en una red y que, a partir de ese momento, disponga de acceso a una amplia gama de recursos de dicha red sin tener que volver a autentificar su identidad. Sería el equivalente a la tarjeta identificativa que se ha de llevar en algunos centros de trabajo. Dependiendo de lo que ponga («visitante» o «investigador»), se podrá acceder a diferentes partes del edificio. Y, al igual que las tarjetas de los centros de trabajo, para conseguir la credencial han de facilitarse otros datos. Así, al llegar al trabajo, se facilita al recepcionista un documento de identidad y, a cambio, éste proporciona una tarjeta identificativa que hay que llevar en todo momento.

La tecnología SSO de mayor implantación es el sistema llamado Kerberos, si bien hay otros muchos sistemas similares —el sistema de Pasaporte de Microsoft, por ejemplo. Existe, además, una fuerte presión para construir tecnologías SSO federadas que vinculen muchos sitios diferentes en Internet. De esta manera, yo podría, por ejemplo, autentificar mi identidad en mi universidad y moverme a continuación a través de cualquier otro dominio federado sin necesidad de volver a identificarme. La gran ventaja de esta arquitectura radica en que puedo autentificar mi identidad en la institución en la que confío sin tener que proporcionar muchos datos personales a otras en las que no confío.

Las tecnologías SSO han sido muy importantes en la construcción de la identidad en Internet, pero hay un segundo tipo de tecnología que creo que se convertirá en la herramienta de identificación más importante de los próximos diez años por dos razones: porque esta alternativa respeta características arquitectónicas importantes de Internet y porque seguirá habiendo una fuerte demanda de mejores tecnologías de identificación. El engorro de teclear nuestro nombre y dirección en cada sitio donde queramos comprar algo quedará atrás. Basta con pensar en el extraordinario aumento de casos de robo de identidad para reconocer que muchos estarían encantados de encontrar algo mejor.

Para comprender este segundo sistema, reflexionemos primero sobre el funcionamiento de las credenciales en el espacio real.[6] El lector tendrá una cartera. En ella probablemente lleve un carné de conducir, tarjetas de crédito, una tarjeta sanitaria, un pase identificativo para el centro de trabajo y, con suerte, algo de dinero. Cada una de las tarjetas mencionadas puede emplearse para autentificar algún hecho acerca del lector —de nuevo, con distintos niveles de fiabilidad. El carné de conducir incluye una fotografía y una lista de características físicas, lo cual es suficiente para comprar alcohol en una licorería, pero no para la NSA. En la tarjeta de crédito aparece la firma de su dueño, y se supone que un vendedor utiliza ese dato para cotejar que quien firma la factura es el titular de la tarjeta. Si el vendedor sospecha que las firmas no casan, podría solicitar al cliente que le mostrara también su carné de conducir.

Fijémonos en las características cruciales de esta arquitectura de «cartera». Primero, estas credenciales son expedidas por diferentes entidades; segundo, el nivel de fiabilidad que ofrecen depende de su tecnología; tercero,

---

6 Para una extraordinaria explicación de esta cuestión, véase Dick Hardt—Etech 2006: «Who Is the Dick on My Site?», 2006, disponible en http://www.identity20.com/media/ETECH_2006.

soy libre de usar estas credenciales de modos que las entidades expedidoras nunca planearon o pretendieron originalmente. Así, el Departamento de Vehículos Motorizados de EEUU nunca se coordinó con la empresa Visa para que sus carnés de conducir fueran empleados por ésta para autentificar la identidad del portador de sus tarjetas; ahora bien, una vez que una credencial es fiable, otra se puede servir de ella. Y cuarto, nada nos exige mostrar todas nuestras credenciales cuando podemos usar sólo una. Es decir, al mostrar nuestro carné de conducir, no revelamos también el número de nuestra tarjeta sanitaria; o al mostrar nuestra tarjeta Visa, no tenemos que mostrar también nuestra tarjeta American Express.

Pues bien, estas mismas características se hallan en el núcleo de lo que puede resultar el añadido más importante a la arquitectura efectiva de Internet desde su nacimiento. Se trata de un proyecto liderado por Microsoft para desarrollar, en esencia, un Metasistema de Identidad —una nueva capa de Internet, una Capa de Identidad, que complementaría las capas de red existentes para agregar un nuevo tipo de funcionalidad. Esta Capa de Identidad no tiene nada que ver con el Pasaporte de Microsoft, ni con ninguna otra tecnología SSO.

Se trata, pues, de un protocolo que posibilita una especie de cartera virtual de credenciales, con los mismos atributos que las credenciales de la cartera analizada —sólo que aún mejor. Esta cartera virtual no sólo será más fiable que la que llevamos en el bolsillo, sino que también nos proporcionará un control más preciso acerca de qué datos personales son revelados a quienes nos los solicitan.

Por ejemplo, en el espacio real, nos pueden robar la cartera fácilmente. Si eso ocurre, hay un periodo de tiempo en que al ladrón le es relativamente fácil usar las tarjetas de crédito para comprar cosas. En el ciberespacio, no resulta tan sencillo robar estas carteras; de hecho, si su arquitectura se diseña bien, sería prácticamente imposible «robarlas». De este modo, una vez que se hurtaran las tarjetas de crédito a su titular, se convertirían en objetos digitales inútiles.

Más aún, en el espacio real, si queremos acreditar que somos mayores de edad y que, por lo tanto, podemos comprar un paquete de seis latas de cerveza, le mostramos al dependiente nuestro carné de conducir para que compruebe nuestra edad. Ahora bien, al hacerlo, le estamos permitiendo conocer también nuestro nombre, nuestra dirección y, en algunos Estados, nuestro número de la Seguridad Social, datos todos de los que no tendría por qué enterarse. En algunos contextos y dependiendo de lo fisgón que sea el dependiente, estos datos son exactamente aquéllos de los que no querríamos que se

enterara. Pero las deficiencias de las tecnologías del espacio real revelan estos datos. Esta pérdida de privacidad es el precio que hay que pagar por hacer negocios.

La cartera virtual sería diferente. Si necesitamos autentificar nuestra edad, la tecnología podría por sí sola autentificar este hecho —es más, podría autentificar simplemente que somos mayores de cierta edad, sin revelar nada más. En caso de que necesitemos autentificar nuestra nacionalidad, tal dato podría certificarse sin revelar nuestro nombre, nuestro número de pasaporte o nuestro lugar de residencia. La tecnología está diseñada para revelar simplemente aquello que deseemos revelar y nada más. (Kim Cameron, uno de los arquitectos principales de este metasistema, afirmaba: «Para mí, ése es el centro del sistema»).[7] Y, lo más importante, usando la potencia de la criptografía, el protocolo posibilita que la otra parte se fíe de lo que revelemos sin requerirnos aportar más datos.

La brillantez de esta solución a los problemas de identificación radica, en primer lugar, en que replica la arquitectura básica de Internet. No hay depósitos centralizados de datos, ni una tecnología de red que todos debamos adoptar. En su lugar, se propone una plataforma de construcción de tecnologías de identidad que, basada en el conjunto TCP/IP, fomente la competencia entre distintos proveedores de privacidad y seguridad. Así, por más que Microsoft encabece el proyecto, cualquiera puede usar este protocolo, que no está vinculado al sistema operativo Windows, ni a ningún otro. Tal y como señala acertadamente Cameron, este metasistema «no puede estar en manos de ninguna compañía ni de ningún país [...] ni tan siquiera puede llevar la impronta de ningún ingeniero».[8]

La Capa de Identidad es una infraestructura para Internet. Tal infraestructura resulta valiosa para (y también suscita preocupación entre) mucha gente aparte de Microsoft. Ahora bien, aunque el trabajo de Microsoft constituya un importante regalo para Internet, la Capa de Identidad no surge por motivos altruistas. «La estrategia de Microsoft se basa en los servicios web», me indicaba Cameron. «Y los servicios web son imposibles sin identidad».[9] Así pues, existe un importante valor público en ella, pero es el interés privado el que está capitaneando el desarrollo de dicho valor público.

---

7 Grabación de audio: entrevista con Kim Cameron (1 de septiembre de 2006, incluido en el archivo con el nombre del autor).

8 *Ibidem*.

9 *Ibidem*.

La Capa de Identidad beneficiaría a los individuos, a los negocios y al Estado, si bien a cada cual de forma diferente. Los individuos podrían protegerse más fácilmente del robo de identidad.[10] Así, si recibimos un correo electrónico de PayPal solicitándonos actualizar nuestra cuenta, sabremos si el emisor es realmente PayPal; o si queremos protegernos contra el *correo basura*, podríamos bloquear todos los correos que no provengan de un servidor autentificado. En ambos casos, la tecnología está aumentando la confianza en Internet y, consecuentemente, reduciendo los perjuicios que se derivan de su falta de fiabilidad —el fraude, principalmente.

El comercio también se beneficiaría de esta forma de tecnología que reduce el fraude y que, al mismo tiempo, proporciona una infraestructura más segura para llevar a cabo transacciones comerciales *online*.

Y finalmente, el Estado se beneficiaría de esta infraestructura de confianza. Si existiera un modo sencillo de requerir a las personas que autentificaran determinados hechos sobre sí mismas, el Estado lo tendría más fácil para insistir en que lo hiciesen. Si resultara más sencillo confirmar que la persona que entró en un sitio web era quien dijo ser, sería mucho más barato proporcionar cierta información a través de la web.

---

10 Numerosos Estados han promulgado ya leyes relacionadas con el robo de identidad. A continuación ofrezco una lista de ellos:

Alabama: Alabama Code § 13A-8–190 por 201
Alaska: Alaska Stat § 11.46.565
Arizona: Ariz. Rev. Stat. § 13–2008
Arkansas: Ark. Code Ann. § 5–37–227
California: Cal. Penal Code § 530.5–8
Connecticut: Conn. Stat. § 53a-129a / Conn. Stat. § 52–571h
Delaware: Del. Code Ann. tit. II, § 854
District of Columbia: Title 22, Section 3227
Florida: Fla. Stat. Ann. § 817.568
Georgia: Ga. Code Ann. § 16–9-120, por 128
Guam: 9 Guam Code Ann. § 46.80
Hawaii: HI Rev. Stat. § 708–839.6–8
Idaho: Idaho Code § 18–3126
Illinois: 720 Ill. Comp. Stat. 5/16 G
Indiana: Ind. Code § 35–43–5-3.5
Iowa: Iowa Code § 715A.8
Kansas: Kan. Stat. Ann. § 21–4018
Kentucky: Ky. Rev. Stat. Ann. § 514.160
Louisiana: La. Rev. Stat. Ann. § 14:67.16
Maine: ME Rev. Stat. Ann. tit. 17-A §905-A
Maryland: Md. Code Ann. art. 27 § 231
Massachusetts: Mass. Gen. Laws ch. 266, § 37E
Michigan: Mich. Comp. Laws § 750.285
Minnesota: Minn. Stat. Ann. § 609.527
Mississippi: Miss. Code Ann. § 97–19–85
Missouri: Mo. Rev. Stat. § 570.223
Montana: Mon. Code Ann § 45–6-332
Nebraska: NE Rev. Stat. § 28–608 y 620
Nevada: Nev. Rev. State. § 205.463–465
New Hampshire: N.H. Rev. Stat. Ann. § 638:26
New Jersey: N.J. Stat. Ann. § 2C:21–17
New Mexico: N.M. Stat. Ann. § 30–16–24.1
New York: NY CLS Penal § 190.77–190.84
North Carolina: N.C. Gen. Stat. § 14–113.20–23
North Dakota: N.D.C.C. § 12.1–23–11
Ohio: Ohio Rev. Code Ann. § 2913.49
Oklahoma: Okla. Stat. tit. 21, § 1533.1
Oregon: Or. Rev. Stat. § 165.800
Pennsylvania: 18 Pa. Cons. Stat. § 4120
Rhode Island: R.I. Gen. Laws § 11–49.1–1
South Carolina: S.C. Code Ann. § 16–13–510
South Dakota: S.D. Codified Laws § 22–30A-3.1.
Tennessee: TCA § 39–14–150 / TCA § 47–18–2101
Texas: Tex. Penal Code § 32.51
Utah: Utah Code Ann. § 76–6-1101–1104
Virginia: Va. Code Ann. § 18.2–186.3
Washington: Wash. Rev. Code § 9.35.020
West Virginia: W.Va. Code § 61–3-54
Wisconsin: Wis. Stat. § 943.201
Wyoming: Wyo. Stat. Ann. § 6–3-901

No obstante, aunque los individuos, el comercio y el Estado se beneficiarían de este tipo de tecnología, también hay algo que cada uno de ellos podría perder.

En este momento, los individuos pueden ser efectivamente anónimos en la Red, pero una plataforma de identidad autentificada les pondría esto mucho más difícil. Imaginémonos, por ejemplo, un desarrollo normativo que bloquee el acceso a un sitio web a todo el que no lleve una señal que, como mínimo, permita seguirle el rastro al usuario —una especie de carné de conducir para Internet. Esa norma, unida a esta tecnología, extremaría las dificultades para expresarse anónimamente en Internet.

Asimismo, el comercio podría perder algo con este diseño. En la medida en que existen mecanismos simples para autentificar que alguien es el usuario autorizado de una tarjeta de crédito, por ejemplo, los sitios web ya no necesitan solicitarle toda clase de datos personales —su dirección, sus números de teléfono e incluso, en un caso que viví recientemente, su fecha de nacimiento. Esto podría llevar a desarrollar una norma contra las peticiones de información superflua, la cual, por otra parte, puede ser valiosa para el comercio más allá de la mera confirmación de un cobro.

E igualmente los Estados pueden perder algo por medio de esta arquitectura de identificación. Como el comercio, el Estado también perdería los datos suplementarios que los usuarios han de revelar para autentificar su identidad. Por más que tales datos pudieran ser necesarios para otros propósitos, su recopilación se haría más difícil.

Cada una de estas ventajas y pérdidas puede ajustarse en función del modo de implementación de la tecnología. Y como la combinación de privacidad y seguridad resultante dependerá de la competencia y del equilibrio entre intereses individuales y comerciales, no hay manera de predecir con ciertas garantías cómo se realizará dicho ajuste.

No obstante, para nuestro interés aquí, el único hecho importante en que hemos de fijarnos es que esta infraestructura podría dar una respuesta efectiva a la primera pregunta que plantea la regulabilidad: ¿*Quién* hizo qué y dónde? Mediante una infraestructura que posibilita la identificación sencilla de alguien dondequiera que esté, el número de actividades no identificadas desciende drásticamente.

Este ejemplo final de tecnología de identificación pone de relieve un hecho importante acerca de la tecnología de cifrado: el hecho de que la Capa de Identidad dependa de la criptogafía demuestra la ambivalencia presente en la misma. Stewart Baker y Paul Hurst lo expresan así: «[La criptografía] es, con toda seguridad, la mejor de las tecnologías que conocemos y, al mismo tiempo, la peor de todas. Impedirá crímenes y, al mismo tiempo, creará otros nuevos. Socavará dictaduras y, al tiempo, las llevará a nuevos excesos. Nos proporcionará a todos anonimato y, al mismo tiempo, seguirá la pista de todas nuestras transacciones».[11]

La criptografía puede hacer todas estas cosas, buenas y malas, porque puede emplearse para dos fines fundamentalmente diferentes. En su función de «confidencialidad» puede ser «usada para mantener en secreto las comunicaciones»; en su función de «identificación», puede ser «usada para procurar identidades digitales a prueba de falsificaciones».[12] Así pues, la criptografía posibilita la libertad con respecto a la regulación (al incrementar la confidencialidad), pero puede también posibilitar una regulación más eficaz (al incrementar la identificación).[13]

Su uso tradicional ha estado vinculado a los secretos: al cifrar un mensaje, sólo aquéllos que poseyeran la clave adecuada podrían abrirlo y leerlo. Este tipo de cifrado ha existido desde los orígenes del lenguaje, pero hasta mediados de la década de los setenta, adolecía de una importante debilidad: la misma clave que se empleaba para cifrar un mensaje se empleaba también para descifrarlo. De resultas, si se extraviaba esa clave, todos los mensajes cifrados con ella podrían quedar al descubierto. Es más, si había un gran número de mensajes cifrados con esa misma clave, la pérdida de la clave comprometería el archivo completo de secretos protegidos mediante esa clave. Este riesgo era muy significativo e implicaba la necesidad de «trasladar» siempre la clave requerida para descifrar el mensaje, con el consiguiente riesgo de perderla en dicho transporte.

---

11 Stewart A. Baker y Paul R. Hurst, *The Limits of Trust: Cryptography, Governments, and Electronic Commerce*, Boston, Kluwer Law International, 1998, p. xv.

12 *Ibidem*.

13 Véase Hal Abelson et al., «The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption», *WorldWideWeb Journal*, núm. 2, 1997, pp. 241, 245: «Aunque tradicionalmente se haya asociado la criptografía a la confidencialidad, otros mecanismos criptográficos, como los códigos de autentificación y las firmas digitales, pueden asegurar que los mensajes no han sido alterados o falsificados».

Sin embargo, a mediados de los setenta, los científicos Whitfield Diffie y Martin Hellman anunciaron un avance capital en la técnica de cifrado.[14] En lugar de basarse en una sola clave, el sistema de Diffie y Hellman empleaba dos claves —una pública y otra privada—, de modo que lo que se cifrara con una sólo pudiera descifrarse con la otra. Incluso aunque se accediera a una de ellas, no habría ningún modo de inferir la otra.

Este avance constituyó la piedra angular de una arquitectura que pudiera incorporar un extraordinario grado de confianza a cualquier red, al margen de la seguridad de la propia red física.[15] Y, de nuevo, tal confianza podría hacer que

14 Whitfield Diffie y Martin E. Hellman, «New Directions in Cryptography», IEEE Transactions on Information Theory IT–22, noviembre de 1976, pp. 29–40. Al parecer, la idea había sido lanzada previamente por James Ellis, del British Government Communication Headquarters (Cuartel general de comunicaciones del gobierno británico) pero no llegó a ser publicada; véase Baker y Hurst, *The Limits of Trust*, op. cit., pp. xvii–xviii.

15 Así, incluso si la red está pinchada, la magia de este tipo de cifrado sigue funcionando. Para llegar a comprender cómo, incluyo a continuación una serie de casos que dejan claro su potencial.

A. Si deseo enviar al lector un mensaje que sé que sólo él será capaz de leer, puedo emplear su clave pública para cifrar mi mensaje. A continuación, puedo enviar ese mensaje al lector sabiendo que sólo el titular de la clave privada (presumiblemente el lector) será capaz de leerlo. Ventaja: el mensaje que envío al lector es seguro. Inconveniente: el lector puede tener dudas de que el remitente sea yo. Como cualquiera puede cifrar un mensaje empleando la clave pública del lector, y enviárselo a continuación, éste no puede tener la certeza de que fuera yo quien se lo envió. Por ello, pasemos a considerar el siguiente ejemplo.

B. Antes de mandarle al lector el mensaje con su clave pública, puedo cifrarlo con mi clave privada. En tal caso, el lector recibe mi mensaje, lo descifra en un primer momento con mi clave pública, para a continuación descifrarlo con su clave privada. Con el primer paso, el lector puede estar seguro de que yo (o el titular de mi clave privada) fui quien se lo envió; con el segundo paso, el lector puede estar seguro de que exclusivamente él (u otros titulares de su clave privada) lee el contenido del mensaje. Pero, ¿cómo sabe el lector que la que yo afirmo que es la clave pública de Larry Lessig es efectivamente la clave pública de Larry Lessig? Es decir, ¿cómo puede estar seguro de que la clave pública que está empleando es la clave pública que se supone que es? Es aquí donde entra nuestro tercer ejemplo.

C. Si existe una tercera parte digna de confianza (mi banco, pongamos por caso, o la Reserva Federal, o la Unión Americana de Libertades Civiles) que disponga de una clave pública (algo que estoy en condiciones de constatar por el prestigio de la institución) y esa tercera parte verifica que la clave pública de Larry Lessig es en verdad la clave pública de Larry Lessig, entonces junto con mi mensaje, cifrado con la clave pública del lector y después con mi clave privada, existiría un certificado expedido por dicha tercera parte y cifrado a su vez con su clave privada. Así, cuando el lector reciba mi mensaje, podrá usar la clave pública de la institución en cuestión para descifrar el certificado; extraer de él mi clave pública (que ahora puede estar seguro que es verdaderamente mía); descifrar el mensaje con la clave extraída del certificado (tras lo cual el lector se cerciora de que yo mandé dicho mensaje); y, por último, descifrar el mensaje cifrado con su propia clave pública (con lo que el lector cuenta con garantía suficiente de que nadie más lo ha leído). Llevando a cabo todo este proceso, el lector sabría que yo soy quien digo ser y que el mensaje proviene de mí; yo sabría que sólo el lector leerá el mensaje; y el lector, a su vez, sabría que nadie más lo interceptará en ruta y lo leerá.

creyera que mis secretos no serían revelados y que la persona que entrara en mi sitio en este instante fuera el lector. La tecnología, por lo tanto, sirve para guardar secretos, pero también lo pone muy difícil; sirve para hacer las cosas menos regulables, pero también permite mayor regulabilidad sobre ellas.

En la primera vida de Internet, la tecnología de cifrado estaba del lado de la privacidad, siendo su uso más común el de mantener información en secreto. Pero en la próxima vida de Internet, el papel más importante de dicha tecnología consistirá en hacer la Red más regulable. A medida que se construye una Capa de Identidad en Internet, aumenta la posibilidad de exigir alguna forma de identidad como condición para acceder a los recursos de la Red. Y a medida que tal posibilidad aumente, aumentará también su predominio. Es más, tal y como describe Shawn Helms, la próxima generación del Protocolo de Internet —Ipv6— «marca cada paquete con una "clave" de cifrado que no puede alterarse o falsificarse, lo cual asegura la identificación del origen del paquete. Esta función autentificadora puede identificar a todo emisor y receptor de información a través de Internet, haciendo así prácticamente imposible mantener el anonimato en Internet».[16]

En cualquier caso, aunque mantener el anonimato en la Red no sea imposible, será lo suficientemente difícil para la inmensa mayoría de nosotros. Por ende, nuestros paquetes estarán marcados, y nosotros —o algo de nosotros— quedará marcado también.

¿Quién hizo *qué* y dónde?

La regulabilidad depende también de conocer el «qué» de la pregunta «¿Quién hizo qué y dónde?». Una vez más, el diseño original de Internet no ayuda al regulador en este sentido. Si el protocolo de Internet simplemente trocea datos en paquetes y marca sobre ellos una dirección, entonces nada en ese protocolo básico revela cuál es su contenido a quien mire el paquete.

16 Shawn C. Helms, «Translating Privacy Values with Technology», *Boston University Journal of Science and Technology Law*, núm. 7, 2001, pp. 288-299.

Por ejemplo, imaginémonos que somos una compañía telefónica que proporciona acceso a Internet de banda ancha (DSL). Algún innovador perspicaz desarrolla un servicio de transmisión de voz sobre IP (VOIP, por las siglas en inglés de *Voice-over-IP*) —una aplicación que permite usar Internet para realizar llamadas telefónicas. A nosotros, la compañía telefónica, esto no nos hace ninguna gracia, pues ahora la gente emplea nuestro servicio DSL para hablar por teléfono sin coste suplementario alguno. Esta libertad conlleva un recorte de nuestros beneficios.

¿Podemos hacer algo al respecto? La respuesta es no, al menos si nos basamos sólo en los protocolos de Internet. Los «paquetes» de datos que contienen las llamadas telefónicas por Internet no se diferencian en nada de cualquier otro paquete de datos, pues no llevan una etiqueta donde se lea «VOIP» o algún otro distintivo congruente. Y es que los paquetes de datos no vienen marcados con explicaciones acerca de su contenido, sino simplemente con direcciones.

Ahora podemos comprender fácilmente, tal y como pretende sugerir mi ejemplo, por qué ciertas instancias estarían ansiosas por averiguar qué es lo que contienen los paquetes que circulan por sus redes, y no sólo con fines anticompetitivos. Los administradores de redes que tratan de decidir si añadir más capacidad necesitan saber para qué se está usando la capacidad existente en ese momento. Las compañías deseosas de evitar que sus trabajadores pierdan el tiempo con los deportes o la pornografía tienen un claro interés en conocer con exactitud qué están haciendo sus empleados. Las universidades que intentan impedir que se instalen virus o programas perjudiciales en sus ordenadores han de conocer qué tipo de paquetes acceden a su red. En todos estos casos, existe una *voluntad* obvia y válida de identificar qué paquetes circulan por las redes. Y, como reza el dicho, querer es poder.

La posibilidad proviene de la misma técnica que se describió en la sección anterior. De nuevo, el protocolo TCP/IP no incluye ninguna tecnología para identificar el contenido de los paquetes TCP/IP. Pero dicho protocolo tampoco interfiere con las aplicaciones que sí podrían examinar los paquetes TCP/IP e informar acerca de su contenido. Así, por ejemplo, un sistema producido por *Ipanema Technologies* habilita al propietario de una red a inspeccionar los paquetes que pasan por ella. Tal y como promete su página web:

> La inspección «profunda» de paquetes a través de la capa siete de Ipanema Systems reconoce automáticamente todos los flujos claves de aplicaciones recreativas y de negocios que circulan por una red. También proporciona interfaces gráficas en tiempo real e informes minuto a minuto para descubrir rápidamente las aplicaciones recién instaladas.[17]

A partir de los datos recopilados mediante esta tecnología, el sistema genera informes acerca de qué aplicaciones se están empleando en una red y por parte de quién. Estas tecnologías posibilitan el control del uso de la red, ya sea para ahorrar costes de banda ancha o para bloquear usos de la red que su propietario no permite.

Otro ejemplo de esta forma de control del contenido es un producto llamado «iProtectYou»,[18] que también inspecciona los paquetes de una red, pero se implementa en los ordenadores de forma particular. Así, los padres instalan este software en un ordenador y éste se encarga de vigilar todo el tráfico de Internet que pasa por esa máquina. Tal y como lo describe la compañía, el programa puede «filtrar sitios web y grupos de noticias perniciosos; restringir el uso de Internet a un horario predeterminado; decidir qué programas pueden disponer de acceso a Internet; limitar la cantidad de datos que puede enviarse o recibirse desde el ordenador; bloquear correos electrónicos, *chats*, programas de mensajería instantánea y conexiones P2P que contengan vocabulario inadecuado; [y producir] registros detallados de la actividad en Internet». De nuevo, nos hallamos ante una aplicación que se instala sobre una red informática para vigilarla. Dicha aplicación interfiere en la actividad de una red cuando identifica en ella la clase de actividad que el administrador quiere controlar.

Junto a estas tecnologías de control, los programadores han desarrollado una amplia gama de dispositivos para vigilar redes. Acaso la aplicación dominante en este contexto sea la llamada «nmap»—un programa:

> Para la exploración de redes o la auditoría de seguridad [...] diseñado para supervisar rápidamente amplias redes [...] nmap emplea de modo novedoso paquetes IP sin procesar para determinar qué anfitriones están disponibles en la red, qué servicios (nombre de la aplicación y versión) están ofreciendo, qué sistemas operativos (incluida su versión) utilizan, qué tipo de filtros de paquetes y de cortafuegos emplean, y otra serie de características.[19]

---

17 Ipanema Technologies, «Automatically discover applications running over your network». Disponible en http://www.ipanematech.com/New/EN/Solutions.php?niv=2a.

18 iProtectYou Pro Web Filter v7.10. Véase http://www.softforyou.com/ip-index.html.

19 Nmap («Network Mapper»). Véase http://www.insecure.org/nmap/.

Esta aplicación es «software libre», lo que significa que su código fuente es «abierto» (público) y que cualquier modificación de dicho código fuente ha de ser igualmente abierta. Tales condiciones garantizan que el código necesario para llevar a cabo esta vigilancia siempre esté disponible.

Finalmente, los desarrolladores han desplegado tecnologías de «filtración de paquetes», que, como describe un ejemplo popular, «consiste en la autorización o el bloqueo selectivo de paquetes de datos en el momento en que pasan a través de un interfaz de red [...] Los criterios usados más habitualmente son la dirección de procedencia o de destino, el puerto de procedencia o de destino, y el protocolo». Estamos de nuevo ante una tecnología que vigila «qué» contienen los paquetes y decide qué está permitido a partir de lo que encuentra.

En ambos casos, una capa de código complementa el protocolo TCP/IP para proporcionar a los administradores de redes algo que el TCP/IP por sí solo no les suministraría —a saber, información acerca de «qué» contienen los paquetes. Esta información incrementa la «regulabilidad» del uso de la red. Si una empresa no quiere que sus empleados se conecten a *chats* de mensajería instantánea, estas tecnologías harán que se cumpla esa regla mediante el bloqueo de los paquetes que contengan dichos *chats*. O si una empresa quiere conocer qué empleados emplean lenguaje sexualmente explícito en sus comunicaciones por Internet, estas tecnologías también se lo revelarán. Una vez más, existen muchas razones perfectamente respetables por las que los administradores de redes pueden querer ejercer esta autoridad reguladora —por más que haya otros muchos casos en los que tal poder sería abusivo—, y esa es la razón de que se desarrolle esta clase de software.

Además, no cabe duda de que existen medidas que los usuarios pueden adoptar para contrarrestar este tipo de vigilancia. Así, un usuario que cifra los datos que envía a través de una red evitará cualquier filtro basado en palabras clave. Junto a ello, abundan las tecnologías diseñadas para facilitar la conducta anónima en Internet, de modo que los administradores no lo tengan fácil para averiguar qué está haciendo alguien en una red. Todas estas medidas, sin embargo, requieren que los usuarios efectúen una importante inversión —ya sea de tiempo o de dinero— y la inmensa mayoría no se tomará esa molestia, con lo que los administradores mantendrán su capacidad de vigilar el contenido y el uso de las redes.

Por lo tanto, al igual que con los cambios que incrementaban la capacidad de determinar «quién» está utilizando una red, aquí también encontramos que los intereses privados proporcionan un incentivo suficiente para

desarrollar tecnologías que hagan cada vez más fácil averiguar «qué» está haciendo el usuario de una red. De resultas, una laguna informativa del diseño original de Internet se completa mediante estas tecnologías de procedencia privada.

¿Quién hizo qué y *dónde*?

Por último, y en la medida en que las diversas jurisdicciones imponen diferentes exigencias, el tercer dato necesario para una regulación eficaz es determinar el lugar donde se encuentra el destinatario de dicha regulación. Si Francia prohíbe la venta de parafernalia nazi, pero EEUU no lo hace, un sitio web que quiera respetar las leyes francesas deberá conocer la procedencia de la persona que accede a su página.

De nuevo nos encontramos con que los protocolos de Internet no proporcionan tales datos, por lo que resulta extremadamente complicado regular o zonificar el acceso al contenido en función de la geografía. En este sentido, un tribunal se pronunció en los siguientes términos acerca del diseño original de Internet:

> Internet es completamente refractaria a distinciones geográficas. En casi todos los casos, los usuarios de Internet ni conocen ni se preocupan por la localización física de los recursos a los que acceden. Los protocolos de Internet se diseñaron para ignorar la localización geográfica, más que para registrarla; así, aunque a los ordenadores de una red se les asignen «direcciones», éstas son direcciones lógicas dentro de una red más que direcciones geográficas en el espacio real. La mayoría de direcciones de Internet no contiene indicio geográfico alguno, y, en caso de que lo contenga, puede resultar engañoso.[20]

Pero he aquí que el comercio viene una vez más al rescate de la regulabilidad. Hay muchas razones obvias por las que sería útil poder identificar dónde está alguien cuando accede a un sitio web. Algunas de ellas tienen que ver con la regulación —bloquear a los franceses el acceso a material nazi

20 American Library Association vs. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997), citado en Michael Geist, «Cyberlaw 2.0», *Boston College Law Review*, núm. 44, 2003, pp. 323, 326–27.

o a los niños el acceso a pornografía— y serán examinadas en profundidad más adelante. Por ahora, sin embargo, las razones que más nos interesan son las puramente vinculadas al comercio, que vuelven a ser suficientes para inducir el desarrollo de esta tecnología.

De nuevo, la ausencia de datos acerca de la localización de alguien es producto del modo en que se diseñaron las direcciones IP. Estas direcciones, al ser virtuales, no remiten a un punto geográfico específico, sino a un punto lógico dentro de una red. De este modo, dos direcciones IP en principio podrían estar muy próximas entre sí en términos numéricos, pero completamente alejadas en términos geográficos, cosa que no sucede con los códigos postales. Así, si el código postal del lector difiere en un solo dígito del mío (94115 y 94116, por ejemplo), podemos pensar que somos prácticamente vecinos.

Ahora bien, esta laguna informativa no es más que una ausencia de datos acerca de la localización de alguien a partir de su dirección IP. Esto significa que, aunque no haya un modo simple de deducir de una dirección del tipo 23.214.23.15 que alguien está en California, ciertamente es posible recopilar los datos que se necesitan cotejar con dicha dirección para localizar a alguien allí. Para ello, se ha de construir una tabla con direcciones IP y puntos geográficos y, acto seguido, seguir la pista tanto de la última dirección IP como del camino recorrido por el paquete desde su punto de partida hasta su destino. En consecuencia, por más que el protocolo TCP/IP no pueda revelar directamente la localización de alguien, puede ser empleado indirectamente para revelar al menos el origen o destino de un paquete IP.

La motivación comercial para acceder a esta información es obvia. Jack Goldsmith y Tim Wu narran la historia de un empresario particularmente famoso, Cyril Houri, que recibió la inspiración de desarrollar tecnologías de mapeo IP sentado una noche en un hotel parisino. Allí, Houri accedió a su cuenta de correo, albergada en un servidor web de EEUU, y se percató de que los *banners* publicitarios de la página estaban anunciando una floristería estadounidense. Esa visión le sugirió una idea (hoy en día obvia): ¿por qué no construir una herramienta que permita a un sitio web saber desde dónde acceden a él, de modo que pueda incluir anuncios geográficamente relevantes para sus usuarios?[21]

---

21 Jack Goldsmith y Timothy Wu, *Who Controls the Internet: Illusions of a Borderless World*, Nueva York, Oxford University Press, 2006, p. 44.

Esta idea de Houri ha sido copiada por muchos desde entonces. Geoselect, por ejemplo, es una empresa que ofrece servicios de mapeo IP. Con sólo acceder a su página web, esta empresa es capaz de determinar automáticamente desde dónde nos hemos conectado con un margen de error de tan sólo un 1 %. Mediante sus servicios, podemos disponer de un informe geográfico que detalla la localización de quienes visitan nuestra página, así como actualizar automáticamente los archivos de registro de nuestro servidor web con datos geográficos. De resultas, tanto la modificación del mensaje de bienvenida de nuestro sitio como el desvío del usuario a otra dirección se efectúa de forma automática en función de su lugar de procedencia. Toda esta funcionalidad resulta invisible para el usuario, que no ve más que una página web construida mediante herramientas que conocen algo que el TCP/IP no revela por sí solo —*su* procedencia.

¿Y qué motivos comerciales tienen los sitios web para emplear este software? Una empresa denominada MaxMind[22] estima que el motivo fundamental es el fraude con tarjetas de crédito: de esta forma, si el cliente de un sitio procede de una «dirección IP de alto riesgo» —esto es, de un lugar que probablemente esté implicado en fraudes con tarjetas de crédito—, el servicio de MaxMind interviene la transacción y obliga a efectuar verificaciones de seguridad suplementarias. Igualmente, MaxMind destaca que sus servicios serán valiosos para una «publicidad orientada al público objetivo», prometiendo a sus clientes que podrán ajustar su mensaje en función del país, el estado, la ciudad, un «código metropolitano», un código de zona e incluso la propia velocidad de conexión del usuario (con lo que se acabó el enviar publicidad de descargas de películas a usuarios con conexión de módem de marcado).

También en este caso existe una importante y potente aplicación de software libre que ofrece los mismos servicios de mapeo IP. Hostip.info proporciona —gratis— a los operadores de sitios web la capacidad de «geolocalizar» a sus usuarios.[23] De nuevo encontramos que la funcionalidad principal del mapeo IP no está exclusivamente en manos de corporaciones o de unas pocas personas. Cualquier programador —incluido el Estado— podría incorporar tal función en sus aplicaciones. El conocimiento y la funcionalidad son libres.

He aquí, pues, que otra laguna informativa original que dificultaba la regulabilidad de la conducta en Internet —la de la identidad geográfica— ha quedado también cubierta; y no por mediación de mandatos estatales u

---

22 Página principal de MaxMind, disponible en http://www.maxmind.com/.

23 Página principal de Hostip.info, disponible en http://www.hostip.info/.

operaciones encubiertas de la NSA (al menos eso espero), sino por el interés comercial de proporcionar aquellos datos que no daba la propia red. De este modo, se incorporan a Internet capas de tecnología que producen los datos que la red necesita.

No obstante, sigue siendo posible eludir la identificación. Seth Finkelstein, activista por las libertades civiles, ha testimoniado la relativa facilidad con que se puede eludir este seguimiento.[24] Pese a todo, tal y como describiré más adelante, un seguimiento puede ser efectivo, incluso si resulta fácilmente eludible. De hecho, cuando dicho seguimiento se coordina con las arquitecturas de identidad descritas previamente, su efectividad se eleva notablemente.

Resultados

En el Capítulo 3, vimos que la irregulabilidad de Internet era producto de su diseño: esto es, que la incapacidad de esa red para identificar quién es un usuario, qué está haciendo y de dónde procede conllevaba que fuera particularmente difícil aplicar las leyes utilizando esa red. No imposible, pero sí difícil. No difícil de aplicar para todos, pero sí para la gente suficiente como para que fuera un problema. El diseño original de Internet proporcionaba a todo el mundo un «Anillo de Gyges», aquél que, como señala Platón en *La República*, volvió invisible a Gyges, el pastor. El dilema de la regulación en un mundo así radica precisamente en el miedo que despertaba este anillo en Platón: con él, «no puede imaginarse que un hombre tenga una naturaleza tan recta como para mantenerse del lado de la justicia».[25]

Y, en el supuesto de que un hombre así eligiera la justicia, pese a disponer del poder del anillo, «la gente le contemplaría como a un idiota de lo más despreciable, por más que en público le alabaran y guardaran las apariencias por miedo a sufrir injusticias».

---

24 Seth Finkelstein, Barbara Nitke y la National Association for Sexual Freedom vs. Ashcroft —Declaración de Seth Finkelstein (última actualización: viernes 28 de abril de 2006), disponible en http://sethf.com/nitke/declaration.php.

25 *Plato's Republic*, Book II, Agoura Publications, Inc., 2001 [ed. cast.: *La República*, trad. por Manuel Fernández-Galiano y José Manuel Pabón y Suárez de Urbina, Madrid, Centro de Estudios Constitucionales, 1970].

Ahora bien, estas lagunas en el diseño original de Internet no tienen por qué mantenerse. Podemos imaginar redes que interactúen fluidamente con Internet pero que no adolezcan de estas «imperfecciones»; y, más importante aún, podemos entender por qué habría un importante interés comercial en eliminar dichas «imperfecciones».

Puede que el lector aún se mantenga escéptico. Por más que la mayoría de la actividad en Internet sea rastreable mediante las tecnologías que he descrito, quizá el lector siga pensando que existen lagunas significativas. No en vano, la explosión del correo basura, de los virus, del robo de identidad y de cosas por el estilo constituye un testimonio importante de que aún quedan muchas conductas que no se pueden regular en Internet. El comercio, actuando por su cuenta, no ha eliminado todavía estas amenazas a sus intereses y a la vida civil. De hecho, ni siquiera está claro que puede llegar a hacerlo, y esto por razones que exploraré más adelante.

Pero no olvidemos que el comercio no es el único actor aquí. El Estado también es un importante aliado y el marco de regulabilidad que el comercio ha construido puede ser perfeccionado por aquél.

En otras palabras, el Estado puede ayudar al comercio, ayudándose a la vez a sí mismo. El próximo capítulo se ocupa de analizar cómo.

5. Regulando el código

El comercio ha cumplido su parte —en beneficio propio e, indirectamente, en beneficio del Estado. Las tecnologías que hacen más eficaz el comercio también hacen más sencilla la regulación. De este modo, aquél respalda a ésta. En este momento, ya hay una gran cantidad de tecnologías que facilitan saber quién es la persona que está conectada a la Red, qué está haciendo y dónde lo está haciendo. Estas tecnologías se construyeron para que los negocios funcionasen mejor, y, con ellas, la vida en Internet es más segura. Ahora bien, el subproducto de este proceso ha sido convertir la Red en un espacio más regulable.

Más regulable no significa perfectamente regulable. Estas herramientas por sí mismas han hecho bastante y, como señala Joel Reidenberg, ya están llevando a los tribunales a reconocer que la conducta en la Red está a su alcance y puede regularse.[1] Sin embargo, no han creado aún los incentivos para implantar la regulabilidad en el corazón de la Red. Ese paso final requerirá la intervención del Estado.[2]

---

1 Joel R. Reidenberg, «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, núm. 153, 2005, p. 1951.

2 Desde la aparición de la primera versión de *El código*, se ha producido un amplio debate acerca de si se necesitará la intervención estatal para hacer efectivos determinados principios públicos importantes. Véase, por ejemplo, Thomas B. Nachbar, «Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character», *Minnesota Law Review*, núm. 85, 2000, p. 215 (sugiriendo que la intervención es necesaria); Neil Weinstock Netanel, «Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory», *California Law Review*, núm. 88, 2000, p. 395 (examinando y enfatizando la deliberación democrática); Jay P. Kesan, «Private Internet Governance», *Loyola University Chicago Law Journal*, núm. 35, 2003, p. 87 (examinando ejemplos fallidos de regulación privada); Thomas Schultz, «Does Online Dispute Resolution Need Governmental Intervention? The Case for Architectures of Control and Trust», *North Carolina Journal of Law and Technology*, núm. 6, 2004, p. 71;

Cuando escribí la primera versión de este libro, ciertamente contaba con que el Estado acabaría dando el paso. Lo acontecido desde 1999 —incluido el nacimiento de la teoría Z que describo más abajo— no ha hecho más que incrementar mi convicción. En EEUU, la identificación de «un enemigo»—el terrorismo— ha debilitado la determinación de resistir a la acción estatal con el fin de aumentar su poder y la efectividad de la regulación. Sigue habiendo un límite, o al menos eso espero, pero no cabe duda de que se ha desplazado. En cualquier caso, poco más necesitaría hacer el Estado para incrementar radicalmente la regulabilidad de la Red. Y estas medidas no despertarían en sí mismas ninguna resistencia significativa. Así pues, el Estado dispone de los medios y del móvil; este capítulo mapea la oportunidad.

El truco es obvio una vez descubierto. Dada la arquitectura de Internet tal y como es, al Estado le puede resultar difícil regular directamente la conducta. Ahora bien, eso no significa que le sea complicado regular la arquitectura de Internet tal y como es. El truco, pues, consiste en que el Estado instigue el desarrollo de una arquitectura que haga más regulable la conducta.

En este contexto, con «arquitectura» no me refiero a la regulación del propio TCP/IP, sino, simplemente, a la que puede modificar las restricciones efectivas de la arquitectura de Internet mediante la alteración del código en cualquiera de las capas dentro de ese espacio. Así, si hay carencia de tecnologías de identificación, la regulación de la arquitectura implica las medidas que el Estado puede tomar para inducir la implementación de tecnologías de identificación.

Si el Estado toma estas medidas, incrementará la regulabilidad de la conducta en Internet. Y dependiendo de lo sustanciales que sean, podría convertir a la Red en el espacio más perfectamente regulable que hayamos conocido. Como describe Michael Geist, «puede que los Estados hayan querido quedarse al margen en la etapa incipiente de la Internet comercial, pero eso se acabó».[3]

Carl Shapiro, «Will Ecommerce Erode Liberty?», *Harvard Business Review*, mayo-junio de 2000, p. 195 (visión optimista acerca del efecto regulador del mercado); Brett Frischmann, «Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market», *Columbia Science and Technology Law Review*, núm. 2, 2000/2001, p. 1 (abogando por la intervención); Cass R. Sunstein, «Code Comfort», *New Republic,* 10 de enero de 2002 (visión optimista acerca de la respuesta del mercado); Henry H. Perritt, Jr., «Towards a Hybrid Regulatory Scheme for the Internet», *University of Chicago Legal Forum*, núm. 215, 2001 (abogando por soluciones privadas respaldadas por el Estado); Jay P. Kesan y Andres A. Gallo, «Optimizing Regulation of Electronic Commerce», *University of Cincinnati Law Review*, núm. 72, 2004, p. 1497 (brillante integración de la teoría de juegos para comprender cuándo se requiere intervención estatal).

3 Michael Geist, «Cyberlaw 2.0», *Boston College Law Review*, núm. 44, 2003, pp. 323-332.

Regular la arquitectura: el ardid regulador

Podemos denominar esto como el «ardid regulador»: en un contexto donde la conducta es relativamente irregulable, el Estado toma medidas para incrementar la regulabilidad. Una vez definido el procedimiento, existe gran variedad de ejemplos que establecen el patrón para aplicar el ardid al ciberespacio.

Congestión de tráfico

Londres tenía un problema de tráfico. Había demasiados coches en el distrito central y no se encontraba el modo de expulsar a los coches «innecesarios».

Así que se tomaron tres medidas. En primer lugar, se ordenó la instalación de matrículas reconocibles mediante videocámara, a continuación, se colocaron videocámaras en tantos lugares públicos como fuera necesario para vigilar —a perpetuidad—qué coches pasaban y dónde eran aparcados.

Hecho esto, a principios de febrero del 2003, se estableció un impuesto de congestión: inicialmente 5 libras al día (entre las 7 de la mañana y las 18:30 de la tarde) para cualquier coche (exceptuando taxis y vehículos residentes que pagaran una tarifa especial), ascendiendo hasta las 8 libras diarias en julio del 2005. Tras 18 meses en marcha, el sistema estaba funcionando «mejor de lo esperado». Las retenciones se redujeron en un 32 %, el tráfico en la ciudad cayó un 15 % y los atascos en las principales carreteras de acceso a la ciudad disminuyeron un 20 %. Actualmente, Londres explora nuevas tecnologías que faciliten aún más la precisión del cobro por el acceso, incluyendo nuevas herramientas de marcado, así como el empleo de tecnologías GPS y GSM que vigilarían los vehículos mientras circulan por la capital londinense.[4]

---

4 Transport for London, «Congestion Charging»; disponible en http://www.tfl.gov.uk/tfl/cclondon /cc_publications-library.shtml; Center for Transportation Studies, «London's Congestion Charge Cuts Traffic Delays, Spurs Bus Use», diciembre de 2004, disponible en http://www.cts.umn.edu/ news/report/2004/12/london.html y en http://www.cts.umn.edu/news/report/2004/12/london.html; Transport for London, «London Congestion Charging Technology Trials», febrero de 2005, disponible en http://www.tfl.gov.uk/tfl/downloads/pdf/congestion-charging/technology-trials.pdf.

Teléfonos

La arquitectura de las redes de telefonía ha experimentado una transformación radical en la última década. Tras resistirse al diseño de Internet durante muchos años,[5] hoy las redes telefónicas están pasando de ser conmutadas por circuitos a ser conmutadas por paquetes. Tal y como ocurre con Internet, los paquetes de información son lanzados a través del sistema y nada asegura que viajen del mismo modo o por la misma ruta. Los paquetes toman la ruta más eficaz, dependiendo de la demanda existente en un momento dado.

Este diseño, sin embargo, crea problemas a la hora de aplicar la ley de forma particular, lo que tiene que ver con el *pinchazo* de teléfonos. En la red conmutada por circuitos, resultaba relativamente simple identificar qué línea había que pinchar; en la red conmutada por paquetes, donde no se puede predecir por qué rutas viajarán los paquetes de datos, se vuelve mucho más complicado pinchar un teléfono.

Al menos, es complicado bajo un diseño determinado de red conmutada por paquetes. Diseños diferentes implicarían dificultades diferentes. Fue este potencial el que llevó al Congreso de EEUU a promulgar en 1994 la CALEA (*Communications Assistance for Law Enforcement Act*, Ley de Asistencia en Comunicaciones para las Autoridades). Este decreto exige que las redes sean diseñadas de modo que las autoridades preserven su capacidad de ejecutar procedimientos de vigilancia electrónica. Dicha exigencia ha sido negociada en el marco de unos acuerdos «de puerto seguro» que especifican los estándares que han de cumplir las redes para satisfacer los requisitos legales.

La CALEA es un ejemplo clásico del tipo de regulación que pretendo resaltar en este capítulo. La industria creó una arquitectura de red; dicha arquitectura no se adecuaba a los intereses del Estado y éste respondió regulando el diseño de la red de modo que sirviera a sus fines. (Por fortuna para las redes, el Estado aceptó, al menos inicialmente, sufragar parte del coste de este reajuste).[6] Como escribe Susan Crawford:

---

5 Véase Katie Hafner y Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet*, Nueva York, Simon and Schuster, 1996, pp. 62–63.

6 La CALEA autorizó la distribución de 500 millones de dólares para costear las modificaciones de los sistemas de telecomunicaciones instalados o implementados antes del 1 de enero de 1995. Se estimó que esta cantidad suponía en torno al 25 % de los costes totales de la modificación. House of Representatives, Subcommittee on Crime, Committee on the Judiciary, Testimony on the Implementation of CALEA. Miércoles 23 de octubre de 1997, testimonio de RoyUSTA (disponible en http://www.fas.org/irp/congress/1997_hr/h971023n.htm).

> Del modo más crucial para el futuro de Internet, las autoridades [...] han dejado claro que quieren asegurarse de que todo nuevo servicio de posible relevancia cumpla con requisitos no especificados de recopilación y transferencia de información antes de ser lanzado. Todo negocio prudente seguirá los dictados de las autoridades, indica el Departamento de Justicia: «Si los proveedores de servicios consideran que su actividad no se ajusta a la CALEA, se les aconseja que busquen asesoramiento a la mayor brevedad, preferiblemente con antelación a la implementación del servicio [...] La negativa del proveedor de servicios a solicitar este asesoramiento sería estudiada seriamente por el Departamento de Justicia en caso de emprender cualquier acción legal».[7]

La CALEA es una «señal», describe Crawford, de que la «FCC puede postular que el diseño de una amplia variedad de servicios, computadoras y sitios web que emplean los protocolos de Internet necesita el permiso de las autoridades estatales. [...] El Estado impondrá membranas de flujo de información como parte del proceso de diseño de productos y servicios *online*».[8] Ese indicio se ha confirmado más adelante: en agosto de 2005, la FCC (*Federal Communications Commission*, Comisión Federal de Comunicaciones) estableció que los servicios de telefonía vía Internet «deben ser diseñados para facilitar las intervenciones de teléfono por parte del Estado».[9]

No cabe duda de que la regulación de la arquitectura de la red no era el único medio al alcance del Congreso. Éste podría haber compensado la merma en la prevención del crimen (al reducirse la capacidad de pinchar teléfonos) mediante un endurecimiento de las penas.[10] O también podría haber aumentado los recursos destinados a la investigación criminal. Ambos cambios habrían alterado los alicientes de los criminales sin recurrir al potencial

---

7 Susan P. Crawford, «Symposium, Law and the Information Society, Panel V: Responsibility and Liability on the Internet, Shortness of Vision: Regulatory Ambition in the Digital Age», *Fordham Law Review*, núm. 74, 2005, pp. 695, 723–24.

8 *Ibidem*, p. 720.

9 Susan P. Crawford, «Someone to Watch Over Me: Social Policies for the Internet», *Cardozo Law School Legal Studies Research Paper*, núm. 129, 2006.

10 Según Richard Posner, presidente del Tribunal de Apelaciones del Séptimo Circuito, esto es precisamente lo que ocurrió cuando el Tribunal Warren sometió el procedimiento criminal a la Constitución. Para compensar la creciente dificultad que entrañaba condenar a un criminal, el Congreso endureció radicalmente las penas criminales. Véase Richard A. Posner, «The Cost of Rights: Implications for Central and Eastern Europe —and for the United States», *Tulsa Law Journal*, núm. 32, 1996, pp. 1, 7–9. El profesor William Stuntz ha defendido una idea similar. William J. Stuntz, «The Uneasy Relationship Between Criminal Procedure and Criminal Justice», *Yale Law Journal*, núm. 107, 1997, pp. 1, 4. La Constitución, en esta historia, actuó como una restricción exógena a la que el Congreso se pudo ajustar. Si las protecciones constitucionales aumentaran, el Congreso podría compensarlo incrementando las penas.

de la red telefónica para seguirles la pista y condenarles. En lugar de eso, el Congreso optó por transformar la arquitectura de las redes de telefonía, usando así directamente las redes para alterar de modo indirecto los incentivos.

Estamos ante un ejemplo de la ley regulando el código. Su efecto indirecto es una mejora en la aplicación de la ley, lograda mediante la modificación de las restricciones que el código le imponía.

Este tipo de regulación funciona bien con las compañías telefónicas, que son pocas y, por eso, relativamente fáciles de controlar. Las compañías telefónicas son, por lo tanto, intermediarios regulables: es probable que las normas dirigidas contra ellas sean efectivas.

Ahora bien, ¿qué sucede cuando los servicios telefónicos (o, mejor dicho, los «servicios telefónicos») comienzan a proveerse a través de Internet; cuando Vonage o Skype sustituyen a la gigante Bell South? ¿Son estas entidades igualmente fáciles de regular?[11]

La respuesta es que sí lo son, aunque por razones diferentes. Skype y Vonage, como otros muchos proveedores de VOIP, buscan maximizar su valor empresarial y éste proviene en parte de demostrar fiabilidad en la regulación de sus operaciones. El incumplimiento de las leyes estadounidenses no constituye una buena base sobre la que construir una empresa saneada y lucrativa. Y eso es tan cierto para la General Motors como lo es para eBay.

Teléfonos: segunda parte

Cuatro años después de que el Congreso promulgara la CALEA, el FBI pidió a la FCC que aumentara aún más el poder regulador del Estado. Una de las enmiendas a la CALEA propuestas por el FBI exigía que las compañías telefónicas revelaran la localización de usuarios de teléfonos móviles,

---

11 Inicialmente, los requisitos de la CALEA se exigieron únicamente a los servicios VOIP proporcionados por compañías propietarias de las redes mediante las que operaban, si bien más recientemente se está presionando para que se extienda al resto de servicios VOIP. Véase Daniel J. Solove, Marc Rotenberg y Paul M. Schwartz, *Information Privacy Law*, (2ª), Nueva York, Aspen Publishers, 2006. Los autores sintetizan la situación en este ámbito en las páginas 287 y 288: «Voice over Internet Protocol (VoIP)».

informando desde qué antena se procesaba una llamada.[12] Los sistemas de telefonía móvil necesitan estos datos para garantizar una conmutación fluida entre los transmisores, y también a la hora de la facturación. Aparte de esto, a las compañías telefónicas tal información no les sirve para nada.

Al FBI, en cambio, esos datos le interesan mucho más y querría acceder a ellos siempre que exista una «razón de orden público legítima». Al requerir su enmienda que las compañías de telefonía móvil proporcionaran dicha información, las obligaba indirectamente a escribir un código que la hiciera accesible.[13]

La motivación original de dicha exigencia resultaba bastante razonable: los servicios de emergencia telefónica necesitaban un modo sencillo de determinar la procedencia de una llamada efectuada desde un móvil. Por lo tanto, la revelación de la localización era necesaria, al menos en esos casos. Pero el FBI deseaba extender el alcance más allá de las llamadas a Emergencias, y presionaron para exigir la recopilación de esta información para cualquier llamada telefónica.

Hasta ahora, las demandas del FBI han tenido éxito con los reguladores y no tanto con los tribunales, si bien los límites impuestos por éstos simplemente elevan la exigencia de la «carga de la prueba» que recae sobre el FBI para acceder a esta información. Sea cual sea el estándar, el efecto de la regulación ha sido obligar a las compañías de telefonía móvil a construir sus sistemas de un modo capaz de recopilar y conservar un tipo de información que sólo sirve al Estado.

---

12 Véase *Federal Communications Commission*, «Further Notice of Proposed Rulemaking», publicado el 5 de noviembre de 1998, en la página 25: «Relativo a: Decreto de Colaboración de las Comunicaciones para la Aplicación de la Ley». (En «J-STD-025 se incluye un parámetro de "localización" que identificaría dónde se halla el "terminal móvil" de un sujeto cuando esta información estuviera razonablemente disponible en el punto de acceso de interceptación y existiera permiso legal para su remisión a las autoridades. La información de la localización estaría disponible para dichas autoridades independientemente de que se empleara un canal de contenidos de llamada o un canal de datos de llamada»). El deseo del FBI de acceder a esta información fue llevado a juicio por grupos de defensa de las libertades civiles y asociaciones del sector. Véase *United States Telecom Association, et al. vs. FCC*, 227 F.3d 450 (D.C. Cir. 2000). El Tribunal permitió que se revelara la información de las antenas de telefonía móvil, pero haciendo recaer sobre el Estado una responsabilidad más sustancial en todo el proceso.

13 Véase *Center for Democracy and Technology*, «FBI Seeks to Impose SurveillanceMandates on Telephone System; Balanced Objectives of 1994 Law Frustrated: Status Report», 4 de marzo de 1999, disponible en http://www.cdt.org/digi_tele/status.html.

Conservación de datos

Las computadoras recopilan datos acerca de cómo son usadas. Estos datos son almacenados en registros, que pueden ser exhaustivos (lo que en inglés se conoce como un *verbose log*) o no —esto es, que pueden almacenar una gran cantidad de datos, o sólo una pequeña porción. Cuantos más datos recopilan, más sencillo resulta rastrear quién hizo qué.

Los Estados están comenzando a reconocer este hecho y hay algunos que se están asegurando de poder aprovecharlo. EEUU está empezando a «sopesarlo»,[14] y el Parlamento Europeo ya ha adoptado una ley para regular «los datos generados o tratados en conexión con la prestación de servicios de comunicaciones electrónicas de acceso público», requiriendo a los proveedores de servicios que conserven datos específicos de utilidad para las autoridades. Ahí se incluyen datos para determinar el origen, el destino, la hora, la duración, el tipo y el equipo empleado en una comunicación específica.[15] Leyes como ésta construirán una capa de rastreabilidad en la plataforma de comunicaciones electrónicas que facilitará a los Estados seguir la pista de la conducta individual. (Del otro lado, en 2006, el congresista de Massachusetts Ed Markey propuso una legislación que prohibiese que determinadas compañías de Internet, sobre todo buscadores, conservasen registros que permitieran rastrear la conducta en Internet.[16] Veremos cuán lejos llega esta propuesta).

---

14 Declan McCullagh, «ISP Snooping Gaining Support», CNET News, 14 de abril de 2006, disponible en http://news.com.com/ISP+snooping+gaining+support/2100-1028_3-6061187.html. El 15 de marzo de 2006, el Parlamento Europeo aprobó una directiva relativa a las obligaciones de conservación de datos que se imponen a los servicios de comunicaciones de disposición pública. Véase Eur. Parl. Doc. (COD/2005/0182). Los congresistas estadounidenses han estado sopesando una legislación similar. Véase Anne Broache, «U.S. attorney general calls for "reasonable" data retention», CNET News, 20/04/06, disponible en http://news.com.com/U.S.+attorney+general+calls+for+reasonable+data+retention/2100-1030_3-6063185.html.

15 Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, disponible en http://register.consilium.eu.int/pdf/en/05/st03/st03677.en05.pdf. Esta directiva europea ha sido transpuesta al ordenamiento jurídico español mediante la aprobación de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. [N. del E.]

16 Declan McCullagh, «Bill Would Force Websites to Delete Personal Info», CNET News, 8 de febrero de 2006, disponible en http://news.com.com/2100-1028_3-6036951.html.

Cifrado

Los ejemplos analizados hasta ahora se han referido a regulaciones que se dirigían a los desarrolladores del código como una manera de modificar indirectamente la conducta. Pero el Estado puede actuar de manera doblemente indirecta: a veces crea incentivos para que sea el mercado el que modifique el código que, de forma indirecta a su vez, modificará la conducta. Un ejemplo sería el fallido intento del gobierno de Bill Clinton de imponer el chip *Clipper* como el estándar para las tecnologías de cifrado.[17]

Ya he esbozado previamente la naturaleza ambivalente de la criptografía: la misma tecnología permite a un tiempo la confidencialidad y la identificación. Lo que le preocupa al Estado es la parte de la confidencialidad. Y es que el cifrado permite a los individuos hacer intraducibles sus conversaciones o intercambios de información para todo aquél que no posea la clave necesaria. Hasta qué punto resultan intraducibles es aún objeto de discusión[18], pero, para nuestra finalidad, bien podemos dar por zanjado el debate afirmando que, para los deseos del Estado, resultan *demasiado* indescifrables. Ante ello, el Estado buscó el control del uso de la tecnología criptográfica tratando de que se aceptara el *Clipper* como estándar para el cifrado.

No es fácil resumir el funcionamiento del chip *Clipper*, pero lo que está claro es que su propósito era fomentar tecnologías de cifrado que dejaran abierta una puerta trasera para el Estado.[19] Una conversación podría cifrarse

---

17 Para una buena discusión sobre la controversia en torno a *Clipper*, véase Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip*, New Haven, Yale University Press, 1997, pp. 32–43. Para una muestra de varios puntos de vista, véase Kirsten Scheurer, «The Clipper Chip: Cryptography Technology and the Constitution», *Rutgers Computer and Technology Law Journal*, núm. 21, 1995, p. 263; cf. Howard S. Dakoff, «The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation», *John Marshall Law Review*, núm. 29, 1996, p. 475. «*Clipper* se adoptó como estándar federal de tratamiento de información para las comunicaciones por voz» en 1994; véase Gurak, *Persuasion and Privacy in Cyberspace, op.cit.*, p. 125.

18 Véase *Electronic Frontier Foundation* (EFF), *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*, Sebastopol (Cal.), Electronic Frontier Foundation, 1998, cap. 1.

19 Para un buen resumen del funcionamiento del *Clipper,* véase Baker y Hurst, *The Limits of Trust, op. cit.*, pp. 15–18; A. Michael Froomkin, «The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution», *University of Pennsylvania Law Review*, núm. 143, 1995, pp. 709, 752–59. Para una discusión más técnica, véase Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* (2ª), Nueva York, Wiley, 1996, pp. 591–93.

de modo que nadie ajeno a ella pudiera entenderla, pero el Estado dispondría de la capacidad (en la mayoría de los casos con una autorización judicial) de descifrarla empleando una clave especial.

La cuestión que se planteó entonces el gobierno de Clinton era cómo se podría extender la implantación de esta tecnología, y al principio pensaron que el mejor modo de lograrlo era simplemente prohibiendo el resto de tecnologías de cifrado. Esta estrategia demostró ser altamente controvertida, por lo que la Administración Clinton recurrió a una técnica diferente: subvencionar el desarrollo e implementación del chip *Clipper.*[20]

La intención era obvia: si el Estado pudiera conseguir que la industria usara *Clipper* porque le salía más barato, entonces podría regular indirectamente el uso de la criptografía. Así, sería el mercado el que impondría la regulación deseada por el Estado.[21]

Sin embargo, el plan de subvenciones falló. El escepticismo acerca de la calidad del código mismo y del secretismo con que se había desarrollado, unido a la oposición frontal a cualquier régimen de cifrado impuesto desde el gobierno (especialmente a uno impuesto por el gobierno estadounidense), empujó a la mayor parte de la industria a rechazar el *Clipper*. Ante ello, la Administración Clinton se vio obligada a tomar otro camino.

Esa alternativa es la más interesante para el propósito de nuestro análisis y es que, durante un tiempo, algunos estuvieron presionando para que las autoridades regularan de forma directa a los desarrolladores del código de cifrado —exigiéndoles que insertaran en ese código una puerta trasera por la que pudiera abrirse paso el Estado.[22] Aunque ha habido una gran variedad de propuestas, todas ellas pretenden garantizar que el Estado disponga de una vía para romper cualquier cifrado que seleccione el usuario.

Comparada con otras estrategias —como prohibir el uso del cifrado o inundar el mercado con un estándar alternativo—, ésta presenta varias ventajas.

---

20 Véase Richard Field, «1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States», *American University Law Review*, núm. 46, 1997, pp. 967, 993.

21 Véase A. Michael Froomkin, «It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow"», *University of Chicago Legal Forum*, 1996, pp. 15, 32.

22 Anick Jesdanun, «Attacks Renew Debate Over Encryption Software», *Chicago Tribune*, 28 de septiembre de 2001, disponible en http://www.chicagotribune.com/technology/local/profiles/sns-worldtrade-encryptionsoftware,0,4953744.story?coll=chi-news-hed.

En primer lugar, a diferencia de la prohibición del uso del cifrado, esta estrategia no interfiere directamente con los derechos de uso de los individuos. En este sentido, no es contradictoria con la reivindicación constitucional, aún no probada, según la cual un individuo tiene derecho a «hablar mediante criptografía». Y esto porque esta estrategia sólo se propone cambiar la gama disponible de tecnologías de cifrado, sin controlar directamente el uso que realiza un individuo. La regulación estatal de la escritura del código de cifrado sería así igual a la regulación estatal del diseño de automóviles: no alcanza a regular el uso individual. En segundo lugar, a diferencia de la técnica de subvencionar una determinada solución del mercado, esta estrategia permite la competencia entre empresas para proporcionar el mejor sistema de cifrado, siempre dentro de los parámetros reguladores dados. Finalmente, a diferencia de ambas soluciones, ésta supone la regulación de sólo un número relativamente reducido de actores, ya que el número de fabricantes de tecnología criptográfica es mucho menor que el de sus usuarios o compradores.

Así pues, al igual que el resto de ejemplos de esta sección, esta solución ilustra cómo el Estado puede regular directamente el código con el fin de conseguir una mejor regulación, si bien indirecta, de la conducta; el Estado emplea la arquitectura del código para alcanzar un propósito sustantivo concreto. En este caso, como en el de la telefonía digital, el propósito consiste en garantizar que la capacidad estatal de inspeccionar ciertas conversaciones no queda anulada por las tecnologías emergentes. Y, una vez más, el Estado persigue ese propósito no regulando la conducta en sí misma, sino regulando las condiciones en las que se da dicha conducta.

Regulando el código para incrementar la regulabilidad

Los cinco ejemplos examinados se refieren a una conducta que el Estado desea regular, pero que no puede (regular fácilmente) de forma directa. Por lo tanto, en todos ellos el Estado regula esa conducta indirectamente mediante una regulación directa de las tecnologías que intervienen. Estas tecnologías, a su vez, restringen la conducta en cuestión de un modo diferente, «influyen en el desarrollo del código»,[23] constituyendo regulaciones del código que, a su vez, hacen más regulable la conducta.

---

23 Jay P. Kesan y Rajiv C. Shah, «Shaping Code», *Harvard Journal of Law and Technology*, núm. 319, 2005, pp. 326–327.

La pregunta que abría este capítulo era si existían maneras por las que el Estado pudiera regular el código de Internet para hacer que la conducta en la Red fuese más regulable. La respuesta obvia es afirmativa. Hay muchas medidas que el Estado podría tomar para hacer más regulable la conducta en la Red, y posee razones obvias para llevarlas a cabo.

Adecuadamente aplicadas, estas medidas reducirían y aislarían la conducta no-rastreable en Internet, aumentando simultáneamente la probabilidad de que la conducta malévola fuera detectada. Este aumento reduciría significativamente los beneficios derivados de dicha malevolencia, expulsando de Internet las malas acciones de una significativa caterva de malhechores.

Por supuesto, esto no funcionaría a la perfección. Ningún esfuerzo de control podrá jamás garantizar perfectamente el rastreo y el seguimiento de la mala conducta. Pero la perfección no constituye el modelo. La pregunta es si el Estado podría ofrecer suficientes incentivos para inducir una transformación de las redes que establezca la rastreabilidad por defecto. Por razones obvias, la respuesta sigue siendo afirmativa.

La forma general

Si el propósito del Estado es facilitar la rastreabilidad, puede lograrlo asociando una identidad a los usuarios de las redes. Un modo concebible de hacerlo sería exigir a los proveedores de servicios que bloquearan las acciones de aquellos individuos que careciesen de un documento de identidad expedido por el Estado. Es improbable, no obstante, que esa estrategia funcionara, puesto que resulta políticamente inviable. Los estadounidenses desconfían hasta tal punto de los documentos nacionales de identidad[24] que sería improbable que aceptaran un carné de identidad para Internet.

---

24 El anterior Fiscal General Richard Thornburgh, por ejemplo, ha calificado la implantanción de un documento nacional de identidad como «una violación de los derechos de los estadounidenses»; véase Ann Devroy, «Thornburgh Rules Out Two Gun Control Options; Attorney General Objects to Registration Card for Gun Owners, National Identification Card», *Washington Post*, 29 de junio de 1989, A41. La Ley de Reforma y Control de la Inmigración de 1986 (Public Law 99–603, 100 Stat 3359 [1986], 8 USC 1324a[c] [1988]) lo descarta en estos términos: «Nada en esta sección deberá interpretarse como una autorización directa o indirecta de la expedición o establecimiento de documentos nacionales de identidad». Teniendo en cuenta el poder de las redes para relacionar

Pero por más que el Estado no pueda *obligar* a los ciberciudadanos a poseer credenciales identificativas, no resulta difícil crear fuertes *incentivos* que les muevan a emplearlas. En EEUU no es obligatorio que todos los ciudadanos posean carné de conducir, pero resulta harto complicado desenvolverse allí sin él, incluso aunque no se conduzca. Las autoridades estadounidenses tampoco exigen llevar encima un documento identificativo de expedición oficial, pero si un ciudadano de EEUU desea volar a otra ciudad, debe mostrar alguno. El razonamiento es obvio: se trata de incentivar tan intensamente el empleo de documentos de identidad en la Red que el Estado acabe por no tener que imponerlos.

Del mismo modo, el Estado podría crear incentivos para favorecer los documentos de identidad digitales, no mediante la regulación directa de los individuos sino mediante la regulación de los intermediarios. Éstos son menos, sus intereses suelen ser meramente comerciales y, por regla general, resultan objetivos de regulación bastante obedientes. Los proveedores de servicios de Internet constituirán así los objetivos «más importantes y obvios» —«puntos focales del control de Internet».[25]

Consideremos en primer lugar los medios con que cuenta el Estado para inducir la extensión de los «documentos de identidad digitales». A partir de aquí, describiré algo más lo que tendrían que ser dichos certificados.

Comencemos, pues, por los medios con que cuenta el Estado:

– Los sitios de Internet pueden condicionar el acceso a ellos en función de si alguien posee o no la credencial adecuada y el Estado dispone del poder para imponerles esta condición. Por ejemplo, el Estado podría exigir que los sitios de juego comprobaran la edad y lugar de residencia de cualquiera que intentara acceder a ellos. A muchos sitios podría requerírseles la comprobación de la nacionalidad u otras credenciales de sus usuarios potenciales. Cuantos más sitios accedieran a estas exigencias, mayor sería el incentivo que

datos, esta protección se me antoja, sin embargo, vacua. Véase también Real ID Act, Pub. L. No. 109–13, Título II, Sección 202, 2005. Esta ley exige que los ciudadanos acudan en persona al Departamento de Vehículos Motorizados y presenten allí varias acreditaciones identificativas, incluyendo la partida de nacimiento, e impone a los consumidores tarifas más elevadas y una verificación de antecedentes penales más estricta. Sus defensores opinan que la ley aborda la relación entre terroristas, inmigrantes ilegales y estándares de identificación.

25 Jack Goldsmith y Timothy Wu, «Digital Borders», *Legal Affairs*, enero/febrero de 2006, p. 44.

tendrían los individuos para poseer las credenciales adecuadas; y cuantas más credenciales poseyeran, más fácil sería imponerles la regulación.[26]

– El Estado podría ofrecer una rebaja de impuestos a aquéllos que presentasen su declaración de la renta con la credencial oficial adecuada.

– El Estado podría establecer un impuesto de un 10% sobre las ventas por Internet y luego eximir de su pago a quienes adquiriesen bienes por medio de un certificado que autentificara su lugar de residencia; así, cuando se informara al Estado sobre la compra, éste podría recaudar el impuesto local correspondiente.[27]

– El Estado podría cobrar a los usuarios por acceder a publicaciones oficiales, a menos que entrasen con el pertinente certificado autentificado en el sitio web donde se encuentren éstas.

– Como ocurre en otras democracias occidentales, el Estado podría imponer el voto obligatorio[28] y a continuación establecer el voto obligatorio por Internet; los votantes acudirían a las urnas virtuales con un documento de identidad digital que certificase que están registrados.

– El Estado podría hacer responsables a las empresas de tarjetas de crédito del coste de cualquier fraude *online* con tarjetas de crédito o débito, siempre que en la transacción no se utilizara el pertinente documento de identidad digital.

---

26 Nótese que esto podría constituir una elusión efectiva de las protecciones que el Tribunal Supremo reconoció en *Reno vs. American Civil Liberties Union*, 117 SCt 2329, 1997. Hay muchas «actividades» en la Red que el Congreso podría regular fácilmente (como el juego). La regulación de tales actividades podría requerir la posesión de un certificado digital de identidad antes de que se permitiera el acceso a los sitios. En la medida en que tal regulación extienda la incidencia de los certificados digitales en el seno de la Red, podría facilitar la justificación de otras condiciones de acceso relacionadas con la expresión.

27 Arthur Cordell y T. Ran Ide han propuesto que se considere un impuesto sobre bits; véase Arthur J. Cordell *et al.*, *The New Wealth of Nations: Taxing Cyberspace*, Toronto, Between the Lines, 1997. Sus argumentos son rotundos desde la perspectiva de la justicia social y económica, pero no tienen en cuenta que un sistema de impuestos de ese tipo requeriría la implantación de una arquitectura que, si es capaz de medir los bits, será capaz de medir también cualquier otra cosa.

28 Entre los países que imponen esta obligación se hallan Argentina, Australia, Bélgica, Grecia, Italia y Suiza; véase Richard L. Hasen, «Symposium: Law, Economics, and Norms: Voting Without Law?», *University of Pennsylvania Law Review*, núm. 144, 1996, p. 2135.

– Y el Estado podría exigir el establecimiento de un registro seguro de servidores de correo electrónico para combatir el correo basura. Esa lista fomentaría que otras entidades comenzaran a exigir un nivel superior de autentificación antes de enviar correos electrónicos. Tal autentificación vendría dada por un documento de identidad digital.

El efecto de cada una de estas estrategias sería el aumento de la importancia de los documentos de identidad digitales hasta que, en algún momento, se alcanzara un punto sin retorno. Para muchos en la Red, resulta obviamente provechoso poder aumentar la confianza en la entidad con la que están tratando, y dichos documentos de identidad digitales contribuirían precisamente a ello. Así, incluso si un sitio permite que se acceda sin ninguna credencial, cualquier paso que se quiera dar más allá de ese contacto inicial podría exigir presentar la identificación pertinente. En adelante, la norma sería navegar en el ciberespacio provisto de un documento de identidad; aquéllos que se negaran encontrarían que la porción del ciberespacio que pueden habitar es muy reducida.

La consecuencia de llegar a dicho punto sin retorno sería la marca efectiva de cada acción que se diera en Internet —como mínimo— con un tipo de huella dactilar digital. Esa huella permitiría a las autoridades —como mínimo— rastrear la acción hasta dar con sus responsables. La ejecución de tal rastreo podría requerir —como mínimo— una supervisión judicial previa. Y esa supervisión podría —como mínimo— seguir los mandatos de la Cuarta Enmienda.

Como mínimo. Y es que la parte crucial de esta historia no es que el Estado pueda fomentar una Internet rica en documentos de identidad: es obvio que puede. En lugar de eso, la cuestión fundamental es qué tipo de Internet rica en documentos de identidad fomentaría el Estado.

Comparemos dos tipos diferentes de documentos de identidad digitales, que podemos comprender recuperando la metáfora de la «cartera» empleada en el capítulo 4, para describir los últimos desarrollos tecnológicos en materia de identidad que Microsoft está liderando.

El primer tipo funcionaría de este modo: cada vez que necesitemos identificarnos, tendremos nuestra cartera y la entidad que demanda dicha identificación hurgará en ella, recopilando cuanta información desee.

El segundo tipo funciona según los parámetros de la Capa de Identidad descrita en el capítulo 4: cuando necesitemos identificarnos, podremos proporcionar la mínima cantidad indispensable de datos.

De este modo, si necesitamos certificar nuestra nacionalidad, sólo revelaremos el dato que lo atestigüe; si necesitamos certificar que somos mayores de edad, actuaremos de igual forma.

A partir de este último modelo resulta posible imaginar un documento de identidad «ultramínimo» —una identificación que no revela nada por sí misma, pero que facilita la rastreabilidad. De nuevo nos hallamos ante una suerte de huella dactilar digital que no significa nada hasta que es descodificada, y que, una vez descodificada, conduce hasta el agente responsable.

Estas dos arquitecturas constituyen los dos extremos de un espectro más amplio. Cada una de ellas acarrea consecuencias radicalmente diferentes para la privacidad y el anonimato. Ninguna de las dos permite el anonimato perfecto, ya que ambas implican como mínimo la rastreabilidad de la conducta. Ahora bien, con el segundo tipo, dicha rastreabilidad puede ser a su vez severamente regulada, y no debería aplicarse para acciones amparadas por la libertad de expresión. Y si se permite dicho rastreo, habrá de ser porque esté respaldado por la autorización judicial pertinente. De esta forma, el sistema conservaría la capacidad de identificar quién hizo qué y cuándo, pero sólo la ejercería en circunstancias autorizadas.

La diferencia entre los dos mundos descritos es, por consiguiente, abismal, y el hecho de que lleguemos a uno u otro depende críticamente de los principios que guíen el desarrollo de esta arquitectura. El primer tipo de documento de identidad digital sería desastroso para la privacidad así como para la seguridad, mientras que el segundo podría incrementar radicalmente ambas, excepto para aquéllos cuya conducta sea legítimo perseguir.

La viabilidad de la introducción por parte del Estado de uno u otro certificado de identidad depende de modo crucial del destinatario de la regulación, de que exista una entidad responsable del código que emplean los individuos que pueda ser efectivamente regulada. ¿Es realmente cierta esta suposición? El Estado puede ser capaz de regular las compañías telefónicas, pero ¿podrá regular a una multitud de desarrolladores de código? Más concretamente, ¿podrá regular a aquéllos cuyo compromiso pasa precisamente por resistirse a ese tipo de regulación?

En un mundo donde los desarrolladores de código fuesen la clase de personas que gobernaban el IETF (*Internet Engineering Task Force*, Grupo de Trabajo en Ingeniería de Internet)[29] de hace unos años, la respuesta probablemente sería negativa. Los héroes mal pagados que construyeron la Red poseen razones ideológicas para resistirse a los mandatos del Estado y no son de los que se pliegan a sus amenazas. Por consiguiente, proporcionan una importante vigilancia del poder estatal sobre las arquitecturas del ciberespacio.

Pero a medida que el desarrollo de código se vuelve comercial —a medida que se vuelve el producto de un número menor de grandes empresas—, la capacidad estatal de regular dicha actividad aumenta. Cuanto más dinero hay en juego, menos inclinados se muestran los negocios (y sus patrocinadores) a asumir los costes de promover una ideología.

El mejor ejemplo lo constituye la historia de la criptografía. Desde el mismo inicio del debate sobre el control estatal de la criptografía, los técnicos han sostenido que tales regulaciones son ridículas, ya que el código siempre puede exportarse y los bits no conocen fronteras. Así pues, argüían, la idea de que una ley del Congreso controlara el flujo de código era absurda.

Sin embargo, lo cierto es que las regulaciones tuvieron un efecto considerable. No sobre los técnicos —que podían conseguir fácilmente tecnologías de cifrado de muy diversos lugares de la Red—, sino sobre las compañías que escribían software que pudiera incorporar tal tecnología. Netscape o IBM no estaban por la labor de construir y vender software que violara la legislación de EEUU, un Estado que mantiene una amenaza bastante enérgica contra estas dos empresas. Tal y como predijeron los técnicos, la regulación no controló el flujo de bits, pero sí que inhibió sustancialmente el desarrollo de software que empleara dichos bits.[30]

---

29 Véase la descripción en Scott Bradner, «The Internet Engineering Task Force», en Chris DiBona *et al*. (eds.), *Open Sources: Voices from the Open Source Revolution*, Sebastopol (Cal.), O'Reilly and Associates, 1999.

30 Michael Froomkin defiende una idea similar: «Las reglas de control de la exportación han tenido un efecto en el mercado doméstico de productos con capacidades criptográficas, como el correo electrónico, los sistemas operativos y los programas de tratamiento de texto. Debido en buena medida a la prohibición de exportar criptografía fuerte, no existe a día de hoy un producto criptográfico estándar de venta masiva en EEUU, pese a que una considerable base matemática y de programación es perfectamente capaz de crear uno»; «It Came from Planet Clipper», *op. cit.*, p. 19.

El efecto ha sido, pues, profundo. Compañías que fueron antaño bastiones de la irregulabilidad se están convirtiendo ahora en productoras de tecnologías que facilitan la regulación. Por ejemplo, Network Associates, heredera del programa de cifrado PGP, fue en sus orígenes una tenaz opositora a la regulación de la criptografía y ahora ofrece productos que facilitan el control corporativo de la criptografía y la restauración de claves.[31] Esta restauración de claves crea una puerta trasera para las empresas que, en muchos contextos, está bastante menos restringida que la puerta trasera estatal.

Cisco Systems constituye un segundo ejemplo.[32] En 1998, Cisco anunció el lanzamiento de un *router* que permitía a los proveedores de servicios de Internet cifrar el tráfico de Internet en el nivel de enlace —esto es, entre puertas de enlace.[33] Ahora bien, este *router* también disponía de un interruptor que, bajo mandato estatal, deshabilitaría el cifrado de los datos del *router* y facilitaría la recopilación de información sobre el tráfico de Internet sin cifrar. En otras palabras, los datos estarían cifrados sólo mientras el Estado lo permitiera.

En ambos casos, la cuestión es que el Estado se convierte en un actor más del mercado de software, determinándolo tanto mediante la creación de leyes como mediante la compra de productos. De una u otra forma, el Estado está influyendo en la oferta de los proveedores de software comercial, que existen para proporcionar lo que demanda el mercado.

Los veteranos de los primeros días de la Red acaso espeten a los proveedores: «¿Cómo habéis podido?».

«Los negocios son así», sería la respuesta obvia.

---

31 Véase «Network Associates and Key Recovery», disponible en http://web.archive.org/web/19981207010043/http://www.nai.com/products/security/key.asp.

32 Cisco ha desarrollado productos que incorporan el uso de cifrado en las capas de red a través del protocolo IP Security (IPSec). Para una breve discusión en torno al IPSec, véase Cisco Systems, Inc., «IP Security–IPSec Overview», disponible en Link 33, http://web.archive.org/web/19991012165050/http://cisco.com/warp/public/cc/cisco/mkt/ios/tech/ security/prodlit/ipsec_ov.htm. Para una más extensa, véase Cisco Systems, Inc., «Cisco IOS Software Feature: Network-Layer Encryption—White Paper»; Cisco Systems, Inc. «IPSec—White Paper», disponibles en http://web.archive.org/web /20020202003100/http://www.cisco.com/warp/ public/cc/techno/protocol/ipsecur/ipsec/tech/ipsec_wp.htm; véase también Dawn Bushaus, «Encryption Can Help ISPs Deliver Safe Services», *Tele.Com*, 1 de marzo de 1997; Beth Davis y Monua Janah, «Cisco Goes End-to-End», *Information Week*, 24 de febrero de 1997, p. 22.

33 Véase la declaración del *Internet Architectural Board* sobre el cifrado «de timbre privado» (*private doorbell*), disponible en http://www.iab.org/documents/docs/121898.html.

El código de la Costa Este y el código de la Costa Oeste

A lo largo de esta sección, he venido hablando de dos tipos de código. Uno es el «código» que promulga el Congreso (como el Código Tributario o el Código Penal). El Congreso aprueba una interminable colección de estatutos que ponen en palabras cómo hemos de comportarnos. Algunos de estos estatutos rigen a las personas, otros a las empresas y otros a los burócratas. La técnica es tan antigua como el gobierno mismo: usa órdenes para controlar. En EEUU, este código se genera fundamentalmente en la Costa Este del país (Washington, DC), por lo que lo denominaremos «código de la Costa Este».

El otro tipo de código es el que «promulgan» los desarrolladores de código —las instrucciones incluidas en el software y en el hardware que hacen funcionar el ciberespacio. Se trata del código en su sentido más moderno, el cual regula según las formas que he comenzado a describir anteriormente. El código de la Red´95, por ejemplo, regulaba con el fin de impedir el control centralizado, y el código de cifrado regula para proteger la privacidad. En EEUU (con la excepción del MIT), este código se genera cada vez más en la Costa Oeste (Silicon Valley, Redmond), por lo que podemos denominarlo «código de la Costa Oeste».

Los códigos de la Costa Oeste y de la Costa Este pueden convivir perfectamente mientras no se presten mucha atención el uno al otro. Esto es, cada uno de ellos puede regular en sus propios dominios. Ahora bien, el argumento de este capítulo es «Cuando el Este y el Oeste se encuentran»: qué sucede cuando el código de la Costa Este descubre cómo el código de la Costa Oeste influye en la regulabilidad y trata de interactuar con él para inducirlo a regular de forma diferente.

Esta interacción ha cambiado. El poder del código de la Costa Este sobre el de la Costa Oeste ha aumentado. Cuando el software era producido por hackers e individuos situados al margen de cualquier institución de control efectivo (por ejemplo, la Universidad de Illinois o el MIT), el código de la Costa Este podía hacer bien poco para controlar el código de la Costa Oeste.[34]

---

34 Poco, pero no nada. Mediante subvenciones de gasto condicionado, el Estado logró inicialmente una alta efectividad en incrementar su participación en la Red, así como en resistirse al desarrollo de tecnologías criptográficas; véase Whitfield Diffie y Susan Eva Landau, *Privacy on*

Pero a medida que el código es producido por empresas, el poder del código de la Costa Este aumenta. Cuando el comercio escribe el código, ese código puede ser controlado, puesto que las entidades comerciales también pueden ser controladas. Por lo tanto, el poder del Este sobre el Oeste aumenta a medida que el código de la Costa Oeste se vuelve cada vez más comercial.

En EEUU existe una dilatada historia de poder que se desplaza del Este al Oeste, una historia que testimonia el choque que se produce entre lo viejo y lo nuevo. El patrón resulta familiar. El Este acecha al Oeste para controlarlo y éste se resiste. Ahora bien, tal resistencia nunca es completa y los principios del Este se integran en el Oeste. Lo nuevo asume algo de lo viejo.

Eso es precisamente lo que está sucediendo en Internet. Cuando el código de la Costa Oeste nació, había poco en su ADN que le llevara a inquietarse en lo más mínimo por los asuntos del código de la Costa Este. La finalidad de Internet era la comunicación punto a punto y la regulación intermedia simplemente se inhabilitó.

Con el tiempo, las preocupaciones de los codificadores del código de la Costa Este se han hecho mucho más acuciantes. Todo el mundo detesta las patologías de Internet —virus, robo de identidad y correo basura, por mencionar sólo las menos controvertidas. Ese aborrecimiento universal ha incitado a los desarrolladores de código de la Costa Oeste a ponerles remedio, con lo que ahora están a merced del influjo que conviene al código de la Costa Este: incorporar complementos a la arquitectura de Internet que lleven a su regulabilidad.

Dicho esto, algunos continuarán resistiéndose a aceptar mi afirmación de que el Estado puede fomentar que la Red sea regulable. Tal resistencia posee una forma común: incluso si emergen estas arquitecturas de identificación, e incluso si se hacen comunes, nada indica que se conviertan en universales, y nada indica que no se las pueda eludir en un momento dado. Los individuos siempre podrán encontrar la forma de sortear estas tecnologías de identificación. Ningún control que se pudiera imponer resultará jamás perfecto.

---

the Line: The Politics of Wiretapping and Encryption, Cambridge (Mass.), MIT Press, 1998. Steven Levy refiere una intervención estatal más directa. Cuando Richard Stallman se negó a proteger bajo contraseña el ordenador del Laboratorio de Inteligencia Artificial del MIT, el Departamento de Defensa amenazó con desconectar la máquina de la Red a menos que se modificara su arquitectura para restringir el acceso a ella. Para Stallman, se trataba de una cuestión de principios; para el Departamento de Defensa, era pura rutina, véase Steven Levy, *Hackers: Heroes of the Computer Revolution*, Garden City (NY), Anchor Press/Doubleday, 1984, pp. 416–418.

Cierto. El control de una Internet rica en certificados de identidad nunca sería completo; siempre existirán escapatorias.

Pero existe una importante falacia en este argumento: que el control perfecto no sea posible no implica que el control efectivo no lo sea. Las cerraduras se pueden forzar, pero eso no implica que no sirvan de nada. En el contexto de Internet, incluso un control parcial produciría efectos significativos.

Aquí, como en otros contextos, opera un principio bovino fundamental. Por más minúsculos que sean los controles, si son aplicados con coherencia, bastarán para dirigir a animales de gran tamaño. Los controles de una Internet rica en certificados de identidad son minúsculos, de acuerdo; pero nosotros somos animales de gran tamaño. Creo, pues, que es tan probable que la mayoría de la gente se resista a estos reguladores de la Red, pequeños pero eficaces, como que las vacas se resistan a las cercas de alambre. Así es como somos y por eso funcionan estas regulaciones.

Así pues, imaginémonos un mundo en el que todos pudiéramos verificar nuestra identidad simplemente mirando una cámara o pasando nuestro dedo por un lector de huellas dactilares. Accederíamos a la Red en sólo un segundo, con un método de validación de nuestros atributos fiable y sencillo, que no dependería de contraseñas fáciles de olvidar o de credenciales fáciles de falsificar.

¿Qué ocurrirá entonces, cuando podamos elegir entre recordar una contraseña y teclearla cada vez que deseemos acceder al ordenador, y simplemente usar nuestro pulgar —o nuestro iris ocular, o aquella parte de nuestro cuerpo que resulte más sencilla de identificar— para acreditar quiénes somos? Cuando lo más fácil sea simplemente revelar nuestra identidad, ¿quién se resistirá a hacerlo?

Si esto es vender el alma al diablo, no nos quepa duda de que la recompensa por hacerlo será extraordinariamente beneficiosa. Imagínese el lector un mundo donde todos sus documentos estén disponibles en Internet en una «red virtual privada», accessible desde cualquier máquina conectada a la Red y perfectamente protegida mediante una clave biométrica.[35] El lector podría sentarse frente a cualquier ordenador, solicitar sus documentos,

---

35 Sobre las redes virtuales privadas, véase Richard Smith, *Internet Cryptography*, Boston, Addison-Wesley, 1997, capítulos 6 y 7; sobre técnicas biométricas de seguridad, véase Fred B. Schneider (ed.), *Trust in Cyberspace*, Washington DC, National Academy Press, 1999, pp. 123–24, 133–34.

realizar sus tareas, responder su correo electrónico y pasar a otra cosa —todo ello de forma perfectamente segura y protegida por una clave validada mediante sus marcas oculares.

Ésta es la arquitectura más fácil y eficaz que se puede imaginar, y su precio (así lo creen algunos) es muy reducido: la autentificación. Tan sólo di quién eres, conéctate a una arquitectura que certifique ciertos hechos acerca de ti, revela tu identidad... y «todo esto será tuyo».

La teoría Z

«Eh, Lessig, al final no ha sucedido lo que predecías. En 1999 afirmaste que el comercio y el Estado trabajarían codo con codo para construir una red perfectamente regulable. Mientras reviso mi bandeja de correo infestada de correo basura, con mi antivirus funcionando de fondo, me pregunto qué piensas ahora. Lo que quiera que fuera posible no ha sucedido. ¿No demuestra eso que estás equivocado?».

Éste fue el mensaje que recibí de un amigo al comenzar este proyecto de actualización de *El código*. Y, por más que yo nunca dije cuándo sucedería el cambio que estaba prediciendo, hay algo interesante en esta crítica. La teoría de *El código* pasa algo por alto: por más incentivos que existan para abocarnos poco a poco a una Red perfectamente regulable, la teoría no explica qué motivaría el paso final. ¿Qué será lo que nos empuje al punto sin retorno?

La respuesta aún no ha sido escrita por completo, pero su introducción se publicó en 2006. En mayo de ese año, la revista *Harvard Law Review* proporcionó 67 páginas al profesor Jonathan Zittrain (de ahí la denominación de «teoría Z») para explicar «La Internet generativa»[36]. El artículo es brillante y el libro que se deriva de él lo es aún más. El argumento que plantea es la pieza que falta en *El código*.

Hay mucho en dicha Internet generativa que le resultará familiar al lector de este libro. Zittrain defiende que los ordenadores de uso general conectados a redes punto a punto han producido una plataforma extraordinariamente

---

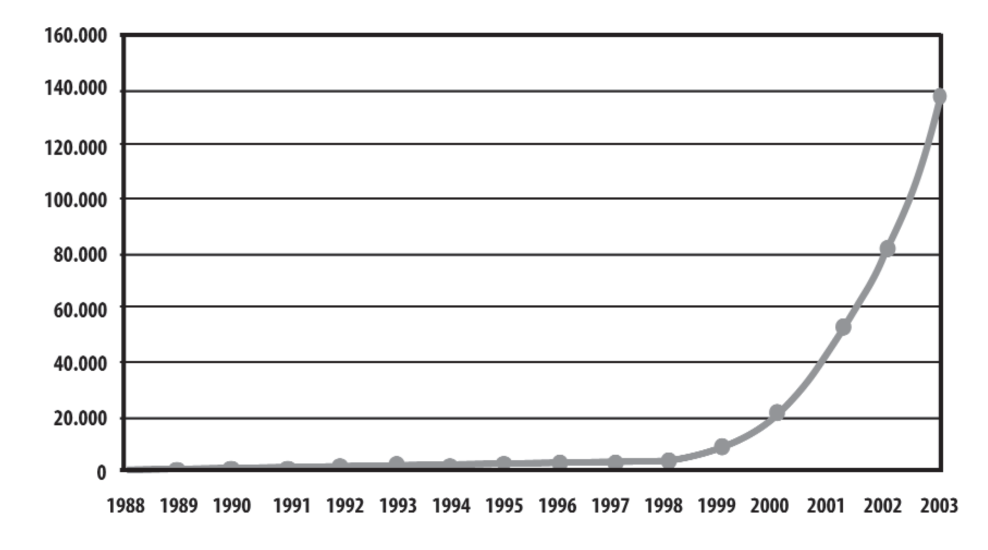
36 Jonathan L. Zittrain, «The Generative Internet», *Harvard Law Review*, núm. 119, 1974, 2006.

innovadora («generativa») para la invención, cuyos logros son dignos de celebración. Ahora bien, los que celebramos esto (yo especialmente) no prestamos suficiente atención a los perjuicios que ha conllevado. Y es que el mismo diseño que permite a un inmigrante indio inventar Hotmail, o a unos inadaptados de la Universidad de Stanford crear Google, también posibilita que haya quien canalice su descontento mediante la creación de virus y otras cosas peores. Este tipo de gente emplea la Internet generativa para hacer daño. Y como Zittrain observa acertadamente, sólo estamos empezando a comprobar cuánto daño provocarán estas creaciones malintencionadas. Analicemos algunos de los ejemplos que ofrece Zittrain al respecto:

– En 2003, en una prueba diseñada para medir el grado de sofisticación de los productores de correo basura para encontrar servidores «de relé abierto» a través de los cuales pudieran enviar su correo sin ser detectados, se encontró que dichos productores daban con el servidor en sólo 10 horas. De esta forma, al cabo de 66 horas habían logrado enviar más de 3,3 millones de mensajes a 229.468 personas.[37]

– En 2004, el gusano *Sasser* fue capaz de poner en peligro más de medio millón de ordenadores —en sólo 3 días.[38] Un año antes, el gusano *Slammer* infectó el 90% de un servidor específico de Microsoft —en sólo 15 minutos.[39]





37 *Ibidem*, p. 2010.

38 *Ibidem*, p. 2012.

39 *Ibidem*.

– En 2003, el virus de correo electrónico SoBig.F fue responsable de casi el 70% de los correos electrónicos enviados mientras se propagaba, incluyendo más de 23,2 millones enviados sólo a usuarios de AOL.[40]

Qué duda cabe de que éstos no son hechos aislados, sino que responden a un patrón que va en aumento. Según las estimaciones del CERT (*US Computer Emergency Readiness Team*, Equipo de Emergencias Informáticas de EEUU), se ha producido una explosión en el número de denuncias que les llegan referidas a incidentes de seguridad. En la página anterior tenemos el gráfico que Zittrain elaboró a partir de la información del CERT.[41]

El gráfico llega a 2004 porque el CERT llegó a la conclusión de que los incidentes estaban tan «generalizados y extendidos que resultaban indistinguibles unos de otros».[42]

El hecho de que en Internet haya programas dañinos no nos sorprende, ni tampoco que su número vaya en aumento. Lo que sí resulta sorprendente es que, al menos hasta el momento, estos programas no hayan provocado la destrucción de la que son capaces. Dada la capacidad de los desarrolladores de este *malware* de infectar con su código malicioso multitud de máquinas en muy poco tiempo, ¿cómo es que nadie más ha intentado hacer daño de verdad?

Imaginémonos, por ejemplo, un gusano que lograse instalarse en un millón de ordenadores, y, en un ataque sincronizado, borrara simultáneamente el disco duro de todos ellos. Zittrain no sostiene que esto resulte sencillo, sino que es tan complicado como lo que vienen haciendo los gusanos que han logrado propagarse por doquier. Así pues, ¿por qué uno de esos desarrolladores de código malicioso no podría causar una verdadera devastación? ¿Qué es lo que evita el Ciberarmagedón?

La respuesta es que no hay una buena respuesta. Y cuando no podemos explicar por qué algo no ha ocurrido todavía, tenemos buenas razones para pensar que llegará a ocurrir. Y cuando ocurra —cuando un autor de software dañino produzca un gusano realmente devastador—, eso provocará que surja la determinación política de llevar a cabo lo que los Estados aún no han completado: presionar para culminar la transformación de la Red en un espacio regulable.

---

40 *Ibidem*.

41 *Ibidem*, p. 2011

42 *Ibidem*.

Ésta es la tesis crucial (y obvia, una vez comprendida) de la teoría Z. El terror desencadena mutaciones radicales. Pensemos, por ejemplo, en los cambios en la aplicación de la ley (y en la protección de los derechos civiles) establecidos en la «Patriotic Act».[43] Esta vasta ley fue promulgada 45 días después de los ataques terroristas del 11-S, pero la mayor parte de su contenido había sido redactado mucho antes de esa fecha. Los autores eran conscientes de que hasta que no se produjera un grave ataque terrorista, no existiría suficiente voluntad política para modificar significativamente el sistema legal. Pero el detonante del 11-S hizo que fuera posible esta modificación radical.

Esto será igualmente cierto con respecto a Internet. Los programas dañinos que hemos conocido hasta ahora han hecho estragos, pero los hemos sobrellevado como algo enojoso, y no amenazador. Ahora bien, cuando llegue el equivalente en Internet al 11-S —sea o no obra de «terroristas»— el enfado se convertirá en voluntad política y ésta producirá un cambio profundo.

El propósito de Zittrain es prepararnos para ese cambio. Su potente y exhaustivo análisis examina las contrapartidas que conlleva la transformación de Internet en un espacio menos generativo. Y pese a que el análisis de su artículo merece por sí solo todo un libro, dejaré que sea él quien lo escriba. Lo que pretendo al incluir esta breve referencia es esbozar una respuesta que complete el rompecabezas teórico de *El código*. Este libro describe los medios, la teoría Z señala el móvil.

En 1996 se estrenó una película espantosa titulada *Independence Day*, que trata de una invasión alienígena de la Tierra. Cuando los extraterrestres aparecen por primera vez, muchos terrícolas están ansiosos por darles la bienvenida. Para estos idealistas no hay razón alguna para mostrar hostilidad, y una alegría generalizada se extiende entre las personas esperanzadas de todo el globo frente a lo que parecía sólo un sueño: existe vida extraterrestre, y «mola».

Sin embargo, poco después de la aparición de los extraterrestres, y en medio de las celebraciones, la actitud previa varía. De repente, los líderes de la Tierra se percatan de que las intenciones de los extraterrestres no son

43 USA PATRIOT ACT (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, Ley para la Unión y Fortalecimiento de América mediante la Provisión de Herramientas Adecuadas Requeridas para Interceptar y Obstruir el Terrorismo), Pub. L. No. 107–56, 155 STAT. 272 (2001); American Civil Liberties Union, *Seeking Truth From Justice: PATRIOT Propaganda —The Justice Department's Campaign to Mislead the Public About the USA PATRIOT Act*, American Civil Liberties Union, 9 de julio de 2003.

nada amistosas. De hecho, son abiertamente hostiles. Pero para entonces ya es muy tarde y los extraterrestres capturan la Tierra. (Sólo Jeff Goldblum se da cuenta a tiempo de lo que sucede, pero es que él siempre se da cuenta de todo antes que nadie).

La historia que expongo aquí es similar (aunque espero que no tan espantosa). Nos hemos mostrado tan acogedores y entusiastas con la Red como los terrícolas de *Independence Day* con los extraterrestres. Hemos aceptado su implantación en nuestras vidas sin cuestionar su efecto final. Pero llegará un momento en que también nosotros vislumbraremos una amenaza potencial, en que comprenderemos que el ciberespacio no garantiza su propia libertad, sino que más bien comporta un extraordinario potencial de control. Y entonces nos preguntaremos: ¿cómo deberíamos responder?

He dedicado muchas páginas a explicar una idea que puede resultar obvia para algunas personas. Pero me he dado cuenta de que, por alguna razón, las personas para las que esta idea debería resultar más importante no la captan. Demasiada gente considera esta libertad como algo dado por naturaleza; demasiada gente cree que la libertad se las arreglará por sí sola; y demasiada gente pasa por alto de qué modo arquitecturas diferentes encarnan principios diferentes, y que sólo escogiendo estas diferentes arquitecturas —estos diferentes códigos— podemos establecer y fomentar nuestros principios.

En este momento, debería quedar claro por qué empecé este libro con un relato del redescubrimiento del papel del autogobierno, o del control, que ha marcado la reciente historia de la Europa postcomunista. Las fuerzas del mercado han fomentado arquitecturas de identificación para facilitar el comercio electrónico. El Estado necesita hacer bien poco —de hecho, no necesita hacer nada en absoluto— para inducir este tipo de desarrollo. Las fuerzas del mercado son demasiado poderosas, y el potencial de este sector es demasiado grande. Si algo es seguro, es que va a desarrollarse una arquitectura de identificación en la Red —transformando así de manera fundamental su regulabilidad.

Ahora bien, ¿no está claro que el Estado debería hacer algo para que esta arquitectura sea coherente con una serie de principios públicos importantes? Si el comercio va a definir las incipientes arquitecturas del ciberespacio, ¿no es cometido del Estado asegurar que aquellos principios públicos que quedan fuera de los intereses comerciales se incorporen también a dicha arquitectura?

La arquitectura es una especie de ley: determina lo que la gente puede hacer y lo que no. Cuando los intereses comerciales determinan la arquitectura, crean una especie de ley privada. Yo no estoy en contra de la empresa privada; de hecho, mi firme opinión en la mayoría de los casos es dejar que el mercado produzca. Ahora bien, ¿no está meridianamente claro que debe haber límites a tal hecho, que los principios públicos no se agotan en aquello que IBM pueda desear, en definitiva, que lo que «es bueno para America Online no es necesariamente bueno para América»?

Por regla general, cuando describimos conjuntos de principios que entran en competencia, así como nuestras elecciones respecto a ellos, calificamos dichas elecciones como «políticas». No en vano se trata de elecciones acerca de cómo se ordenará el mundo y de qué principios se priorizarán sobre el resto.

Las elecciones entre principios, las elecciones acerca de la regulación, del control y de la definición de espacios de libertad —todas ellas corresponden al ámbito de la política. El código «codifica» principios y, sin embargo, la mayoría de la gente habla como si el código fuese meramente una cuestión de ingeniería; o como si fuese mejor dejarlo en manos del mercado, sin que el Estado influya sobre él.

Pero estas actitudes son erróneas. La política es el proceso por el que decidimos colectivamente cómo deberíamos vivir. Esto no equivale a afirmar que es un espacio donde colectivizamos —un colectivo puede optar por una forma de gobierno liberal. Lo importante de la política no radica en la sustancia de la elección, sino en el proceso. La política es el proceso por el que razonamos sobre cómo deberían ser las cosas.

Hace dos décadas, en una pujante trilogía que concitó todo un movimiento en el ámbito de la teoría legal, Roberto Unger preconizó que «todo es política».[44] Según él, no deberíamos aceptar que nada de lo que define el mundo sea desgajado de la política —todo debería considerarse «en tela de juicio» y susceptible de reforma.

Muchos creyeron que Unger sostenía que deberíamos poner en tela de juicio todo durante todo el tiempo, que nada debería ser cierto o fijo, que todo debería fluir constantemente. Pero no era eso lo que quería decir.

---

44 Roberto Mangabeira Unger, *Social Theory: Its situation and Its Task*, Nueva York, Cambridge University Press, 1987.

Lo que Unger quería decir era, simplemente, que deberíamos cuestionar las necesidades de cualquier orden social específico y preguntarnos si constituyen realmente necesidades; y que deberíamos exigir que dichas necesidades justifiquen los poderes que gobiernan en la práctica. Tal y como lo expresa Bruce Ackerman, ante todo ejercicio de poder hemos de preguntar: ¿por qué?[45] Quizá no exactamente en el momento en que se ejerce el poder, pero sí en algún momento.

En este sentido, «poder» no es más que otra palabra para referirse a las restricciones sobre las que los humanos podemos intervenir. Los meteoritos que se estrellan contra la Tierra no son «poder» en el contexto de la afirmación «todo es política». El lugar donde impacta el meteorito no incumbe a la política, si bien las consecuencias de dicho impacto pueden muy bien hacerlo. Y es que el lugar donde impacta el meteorito es algo que va más allá de la acción humana.

Pero la arquitectura del ciberespacio sí es poder en este sentido: podría ser diferente a como es ahora. La política se ocupa de cómo decidimos, del modo en que se ejerce ese poder y de quién lo ejerce.

Si el código es la ley, entonces, como escribe William Mitchell, «el control del código es poder»: «Para los ciudadanos del ciberespacio, [...] el código [...] se está convirtiendo en un foco crucial de lucha política. ¿Quién escribirá el software que estructura cada vez más nuestra vida cotidiana?».[46] Tal y como es el mundo actual, los desarrolladores de código se convierten progresivamente en legisladores. Determinan cómo será Internet por defecto; si la privacidad estará protegida y hasta qué punto se permitirá el anonimato y se garantizará el acceso. Ellos son quienes establecen su naturaleza. Sus decisiones, de momento tomadas en los resquicios de la codificación de la Red, definen lo que es Internet.

Cómo regula el código, quiénes son sus desarrolladores y quién los controla —he aquí tres interrogantes sobre los que cualquier práctica de justicia debe centrarse en la era del ciberespacio. Las respuestas revelan el modo en que está regulado el ciberespacio. Lo que sostengo en esta parte del libro es que el ciberespacio está regulado por su código y que dicho código está cambiando.

---

45 En Bruce Ackerman, *Social Justice in the Liberal State*, New Haven, Yale University Press, 1980, el dispositivo analítico esencial es el diálogo: toda afirmación de poder se enfrenta a una exigencia de justificación [ed. cast.: *La justicia social en el estado liberal*, rev. por Luis Rodríguez Abascal y trad. por Carlos Rosenkrantz *et al*., Madrid, Centro de Estudios Constitucionales, 1993].

46 William J. Mitchell, *City of Bits: Space, Place and the Infobahn*, Cambridge (Mass.), MIT Press, 1996, p. 112.

Estamos entrando en una era en la que el poder regulador se desplazará a una estructura cuyas propiedades y posibilidades son fundamentalmente diferentes. Como señalé al comienzo respecto a Rusia, puede que se destruya una forma de poder, pero otra viene a reemplazarla.

Nuestro objetivo debe ser comprender este poder y preguntarnos si se ejerce adecuadamente. Tal y como pregunta David Brin: «Si admiramos la Red, ¿no debería recaer la "carga de la prueba" en aquéllos que quieren cambiar los supuestos básicos que dieron lugar a la Red en un primer momento?».[47]

Dichos «supuestos básicos» se fundaron en la libertad y la apertura. Ahora una mano invisible amenaza ambas y necesitamos comprender cómo.

Un ejemplo de las luchas abiertas en torno a las ciberlibertades es la *todavía-no-libre* China. El Estado chino ha asumido una postura cada vez más agresiva contra las conductas en el ciberespacio que vulneren las normas del espacio real. Los proveedores de pornografía son condenados a 10 años de cárcel, al igual que los críticos con el gobierno. En la República Popular China, el amor al pueblo puede llegar a matar.

Para posibilitar la aplicación de estas penas, el Estado chino necesita la ayuda de los proveedores de servicios de Internet. Y las leyes locales obligan a dichos proveedores a prestarse a colaborar. De este modo, no dejan de aparecer noticias que informan de que grandes compañías de Internet —incluyendo Yahoo! y Microsoft— colaboran con el Estado chino para llevar a cabo la clase de cosas que resultan execrables en el marco de nuestra Constitución.

Los extremos nunca son buenos. Pero el ejemplo más revelador del patrón regulador que vengo describiendo lo constituye Google. Google es una empresa que disfruta de una fama (merecida) por su fantástico motor de búsqueda y que se ha forjado una imagen de no condicionar los resultados de sus búsquedas en función de factores irrelevantes. Las compañías pueden comprar palabras de búsqueda, pero los resultados derivados de dicha compra aparecen entre paréntesis y separados de los resultados principales —esa zona de la pantalla a la que se dirige instintivamente nuestra mirada—, que se nos presentan así sin interferencias.

---

47 David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Boulder, Perseus, 1999, p. 324.

Eso sí, siempre que la compañía que trate de interferir los resultados no sea China, SA, para la que Google ha prometido construir una rutina especial.[48] Los sitios web que China desee bloquear no se mostrarán en el motor de búsqueda google.cn, y el usuario no recibirá ningún aviso informándole de que los resultados de su búsqueda han sido filtrados por los censores chinos. En lugar de eso, la página de Google aparecerá ante el internauta chino como si nada anormal ocurriera. Y como Google es tan genial, el Estado chino sabe que muchos seguirán recurriendo a su motor de búsqueda incluso aunque Google filtre lo que el Estado no quiere que el pueblo conozca.

He aquí el matrimonio perfecto entre comercio y Estado. Google puede construir la tecnología que China necesita para aplicar mejor sus leyes, y China puede sacar partido de ese talento imponiendo esas leyes como condición de acceso al mercado chino.

Por consiguiente, el valor de ese mercado es más importante para Google que el valor de su principio de «búsqueda neutral». O al menos, más le vale, si es que ese trato tiene algún sentido.

Mi propósito aquí no es criticar a Google —ni a Microsoft, ni a Yahoo!. Estas compañías se rigen por los intereses de sus accionistas; su misión consiste en maximizar su valor corporativo. Si yo estuviera a cargo de cualquiera de esas compañías, no estoy seguro de que hubiera actuado de modo diferente.

Pero en eso consiste precisamente mi argumento: el comercio se debe a unos intereses y el Estado puede explotar eso en su propio beneficio. Podemos estar seguros de que lo hará, cada vez más y cada vez más a menudo, y cuando lo haga, el carácter de la Red se transformará.

Y lo hará radicalmente.

---

48 Ahora bien, este plan sigue rodeado de incógnitas. En junio de 2006, el cofundador de Google Sergey Brin expresó algunas dudas sobre los planes de Google. Véase Thomas Crampton, «Google Is Voicing Some Doubt Over China», *International Herald Tribune*, 7 de junio de 2006.

Segunda parte

Regulación mediante código

La lección de la última parte fue que la interacción entre comercio y Estado cambiará, en la práctica, la arquitectura de Internet, incrementando la regulabilidad de la conducta en la Red. Se esparcirá polvo sobre los hombres invisibles del ciberespacio y, tras ello, sus proezas serán más fáciles de reconocer.

Hasta ahora, no obstante, mi historia sólo ha hablado del modo básico por el que el Estado regula: amenaza con un castigo y dicha amenaza pretende crear el incentivo para que los individuos obedezcan sus reglas. Los cambios en la arquitectura del ciberespacio que he descrito simplemente le facilitarían la capacidad para cumplir su amenaza, y esto reduciría (a ser posible, a un nivel por debajo de cero) el valor que se espera obtener de la conducta criminal. La rastreabilidad incrementará la aplicación de la ley y ésta, los costes de incumplir una regla emanada del Estado.

En esta parte, tomo en consideración un tipo diferente de regulación. La cuestión aquí no es cómo la arquitectura de la Red facilitará la regulación tradicional, sino cómo dicha arquitectura de la Red —o su «código»— deviene ella misma un regulador. En este contexto, la fuerza de la regla que se aplica a un individuo no proviene de la amenaza de las consecuencias impuestas por la ley —multas, cárcel o incluso la propia vergüenza—, sino que su aplicación se apoya en una especie de física. Una puerta cerrada con llave no es una orden

de «No entrar» respaldada por la amenaza del castigo estatal, sino un obstáculo físico a la libertad de alguien para entrar en algún sitio.

Lo que defiendo aquí es que esta forma de regulación será cada vez más común en el ciberespacio, y que, además, posee un carácter distintivo y a menudo contrario a la intuición. El propósito de esta parte consiste en explorar este modo distintivo de regulación como un paso hacia una comprensión más sistemática de la interacción entre tecnología y política.

6. Ciberespacios

PREVIAMENTE HE DICHO QUE PODEMOS DISTINGUIR INTERNET del ciberespacio. Pues bien, para resaltar la forma distintiva de regulación de la que se ocupa esta parte, necesitamos decir algo más sobre esta diferencia. Internet es un medio de comunicación. La gente hace cosas «en» Internet, cosas que son en su mayor parte triviales, por más que no dejen de tener importancia. En Internet, la gente paga facturas, reserva mesa en restaurantes, consulta noticias o se comunica con sus familiares mediante correo electrónico o mensajería instantánea. Estos usos son importantes en el sentido de que afectan a la economía y hacen la vida más fácil o más difícil, pero no en el sentido de que alteren el modo en que vive la gente. Está muy bien eso de comprar en Amazon con un solo clic. Yo mismo compro toneladas de libros (quizás literalmente) que, de otra manera, no habría comprado, pero mi vida no ha cambiado en un clic de ratón (aunque mi cuenta bancaria sí). Tan sólo se ha hecho más fácil y erudita, pero no diferente en sus fundamentos.

El ciberespacio, en contraste, no se limita a hacer la vida más fácil: la hace diferente, o quizás mejor, dando lugar a una vida distinta (una *segunda vida*). El ciberespacio evoca, o engendra, maneras de interactuar que antes no eran posibles. No quiero decir que la interacción sea nueva —siempre hemos tenido comunidades; estas comunidades siempre han producido algo similar a lo que describiré como producto del ciberespacio. Sin embargo, estas comunidades virtuales crean una diferencia de grado que ha evolucionado hasta convertirse en una diferencia cualitativa. Hay algo único en las interacciones que se dan en estos espacios, y algo especialmente único en la forma en que se los regula.

La vida en el ciberespacio está regulada primordialmente mediante el código del ciberespacio. No regulada en el sentido que examinamos en la primera parte —no digo que el código haga más fácil saber quién hizo qué para que los infractores puedan recibir sus penas—, sino en el sentido en que los barrotes de una prisión regulan el movimiento de un preso, o en que las escaleras regulan el acceso para las personas con discapacidad. El código es un regulador en el ciberespacio porque define los términos en que éste se nos ofrece. Y aquéllos que establecen dichos términos reconocen cada vez más el código como un medio para conseguir las conductas que más les benefician.

Y lo mismo sucede con Internet. En la Red, el código también es un regulador, y la gente vive su vida en Internet según esa regulación. Ahora bien, mi estrategia en este capítulo es comenzar por la parte más oscura para después reconocer la parte que nos es familiar. Una vez que captemos la técnica que se aplica a mundos donde es improbable que habitemos, reconoceremos la que se aplica al mundo que habitamos todo el tiempo.

El ciberespacio no es un solo lugar, sino muchos. Y las características de estos lugares difieren de modos que son fundamentales. Estas diferencias proceden, en parte, de las diferencias de la gente que los puebla, pero la demografía por sí sola no explica la discrepancia. Algo más está ocurriendo.

Le propongo una prueba al lector. Lea el siguiente pasaje y pregúntese si la descripción le suena familiar:

> Estoy convencido de que las comunidades virtuales prometen restituir a los estadounidenses de finales del siglo XX lo que muchos de nosotros sentimos que se perdió en las primeras décadas del siglo —un sentido estable de comunidad, de lugar. Pregúntele a aquéllos que han sido miembros de una de estas comunidades virtuales, y le contarán que lo que ocurre allí es más que un intercambio de impulsos electrónicos a través de cables. No se trata meramente de fiestas virtuales [...] También hay que considerar lo reconfortado que se siente un hombre como Phil Catalfo cuando se queda despierto hasta altas horas de la madrugada cuidando de su hijo con leucemia, y se conecta a WELL y vuelca allí su angustia y sus miedos. La gente realmente se preocupa por los demás y se enamora a través de Internet, del mismo modo que lo hace en las comunidades geográficas. Y esa vinculación «virtual» es un signo real de

> esperanza en una nación cada vez más abrumada por la fragmentación de la vida pública, la polarización de grupos de interés y la alienación de la existencia urbana.[1]

Una declaración de esta índole despierta dos tipos de reacciones. A aquéllos que han pasado un cierto tiempo en el «ciberespacio» les resulta extremadamente familiar; han frecuentado diferentes clases de «redes» desde los primeros tiempos, trasladándose a Internet desde comunidades más aisladas —desde un BBS (*bulletin board service*, servicio de tablón de anuncios) local, o desde lo que Mike Godwin (el autor del pasaje anterior) denomina una dirección *chic* como WELL.[2] Para ellos, la Red es un espacio para conversar, entablar contactos e intercambiar ideas —un sitio extraordinariamente prometedor para hacer diferente la vida en el espacio real.

Ahora bien, es muy probable que tal declaración impaciente a los recién llegados a este «espacio» (los veteranos les llaman «novatos»), o a aquéllos que sólo se conectan a Internet para revisar sus cuentas o consultar los horarios del

---

1 Mike Godwin, *Cyber Rights: Defending Free Speech in the Digital Age*, Nueva York, Times Books, 1998, p. 15. Véase también Esther Dyson, *Release 2.0: A Design for Living in the Digital Age*, Nueva York, Broadway Books, 1997, donde se afirma: «Usada correctamente, Internet puede ser una potente tecnología que fomente el desarrollo de comunidades, puesto que da pie a lo que crea una comunidad —la interacción humana» (p. 32) [ed. cast.: *Realease 2.0*, trad. por Ana Alcaina Pérez, Madrid, Punto de Lectura, 2000]. Véase también Stephen Doheny-Farina, *The Wired Neighborhood*, New Haven (Conn.), Yale University Press, 1996, pp. 121–137. Para una importante recopilación donde se examina la comunidad en el ciberespacio, véase Marc A. Smith y Peter Kollock, *Communities in Cyberspace*, Nueva York, Routledge, 1999. Esta recopilación abarca aspectos sociales de la comunidad, incluyendo «orden social y control», «acción colectiva», «estructura y dinámica comunitarias» e «identidad» y la misma relación entre arquitectura y normas que expongo en este capítulo orienta buena parte de su análisis [ed. cast.: *Comunidades en el ciberespacio*, trad. por José María Ruiz Vaca, Barcelona, Editorial UOC, 2003].

2 En 1968 el influyente investigador-activista-artista estadounidense Stewart Brand lanzó (junto a su mujer, Lois Jennings, un pequeño grupo de amigos y algunos colaboradores del Portola Institute, un foro educativo alternativo radicado en Menlo Park, California) el primer número de la revista *The Whole Earth Catalog* (*el catálogo de toda la tierra*). En sus veinticuatro años de irregular publicación, se convertiría en referencia indispensable de buena parte de los movimientos sociales californianos y estadounidenses, representando una fuente de inspiración para varias generaciones por ser fiel, en todas sus dimensiones, al espíritu de experimentación *low-tech* y de autonomía creativa que en aquella época quedaba resumido en la expresión: *Ask not what your country can do for you. Do it yourself* («No preguntes qué puede hacer tu país por ti. Hazlo tú mismo»). En 1985, Stewart Brand y Larry Brilliant crean la pionera comunidad virtual WELL (*Whole Earth 'Lectronic Link*, Enlace electrónico de toda la Tierra) como un trasvase a la naciente red informática de la visión mundial del Catálogo. Este célebre foro electrónico ha reunido hasta hoy a numerosos científicos, estudiosos, activistas, periodistas y demás personas interesadas en temáticas que van desde los deportes hasta la espiritualidad, la política y la programación. Su lema *You Own Your Own Words* («Tú te responsabilizas de lo que dices») ha supuesto una referencia indispensable para posteriores comunidades virtuales. [N. del E.]

cine. Cuando éstos escuchan hablar de «comunidad», de formas especiales de conexión o del asombroso poder de este espacio para alterar las vidas, probablemente se preguntan: «¿De dónde ha salido esta idea de que el ciberespacio es un lugar?». Para los novatos, los que simplemente utilizan el correo electrónico o navegan por Internet, eso de la «comunidad» de la Red es sólo un tipo extravagante de misticismo. ¿Cómo puede alguien considerar que esas páginas rebosantes de anuncios e iconos giratorios constituyen una comunidad, o incluso un espacio? Para el novato comedido, esto suena al furor desatado por el Java.[3]

Los novatos conforman hoy por hoy la mayoría silenciosa de la Red.[4] Por más que uno idealice los viejos tiempos en que la Red era un lugar para la conversación y el intercambio, ésta no es la función que le da la mayoría de sus usuarios. Existen efervescentes comunidades de creatividad y de *blogueros*, pero éstos representan sólo un 3% de los usuarios de Internet; la inmensa mayoría de los usos de la Red carece de conexión con cualquier ideal de comunidad.

El ambiente del ciberespacio ha cambiado.[5] Su apariencia, lo que se puede hacer allí y la forma de conectarse a él —todo esto ha cambiado. Por qué ha cambiado constituye una pregunta complicada —para la cual carezco

---

3 Tal y como exploré en la primera versión de *El Código*, la reciente dimensión «comunitaria» de la Red podría constituir una considerable fuente de negocio. Numerosas obras influyentes han defendido que la clave del éxito del comercio electrónico radica en el desarrollo de «comunidades virtuales»; véase, por ejemplo, Larry Downes y Chunka Mui, *Unleashing the Killer App: Digital Strategies for Market Dominance*, Boston, Harvard Business School Press, 1998, pp. 101–109 [ed. cat.: *Killer app: estratègies digitals per a dominar el mercat*, trad. por Roser Soms Tramujas, Barcelona, Editorial Pòrtic, 2000]. John Hagel y Arthur G. Armstrong, *Net Gain: Expanding Markets Through Virtual Communities*, Boston, Harvard Business School Press, 1997 [ed. cast.: *Negocios rentables a través de Internet: Net Gain*, trad. por Florentino Heras Díez, Barcelona, Paidós Ibérica, 2000]. La explosión que se ha dado desde entonces de entidades esencialmente basadas en comunidades, como la Wikipedia o MySpace, confirma la visión de estos autores.

4 Para un estudio detallado de la demografía de Internet, véase E-Consultancy, *Internet Statistics Compendium*, 12 de abril de 2006, disponible en http://www.e-consultancy.com/publications/internet-stats-compendium/.

5 Para hacerse una buena idea de cómo era antes, véanse los artículos de Rheingold, Barlow, Bruckman y Ramo incluidos en la parte 4 de Richard Holeton (ed.), *Composing Cyberspace: Identity, Community, and Knowledge in the Electronic Age*, Boston, McGraw-Hill, 1998. El libro de Howard Rheingold (cuyo primer capítulo aparece citado en el libro de Holeton) es también un clásico temprano; véase *The Virtual Community: Homesteading on the Electronic Frontier*, Reading (Mass.), Addison-Wesley, 1993 [ed. cast.: *La comunidad virtual: una sociedad sin fronteras*, trad. por José Ángel Álvarez, Barcelona, Gedisa, 1996]. El libro de Stacy Horn es un texto brillante surgido de forma más directa del intercambio (y de otras cosas) en la Red; véase *Cyberville: Clicks, Culture, and the Creation of an Online Town*, Nueva York, Warner Books, 1998.

de una respuesta completa. El ciberespacio ha cambiado en parte porque la gente —sus identidades e intereses— también lo ha hecho, y, por otro lado, porque han variado las posibilidades que brinda el propio espacio.

Parte de dicho cambio, no obstante, está relacionado con el espacio en sí mismo. Comunidades, intercambio, conversación, todo eso florece en un cierto tipo de espacio y se extingue en otro distinto.[6] Mi esperanza es poder iluminar las diferencias entre esos dos entornos.

Las siguientes secciones describen diferentes ciberlugares con el propósito de construir intuiciones sobre cómo hemos de examinar las diferencias que observamos. Estas intuiciones, a su vez, nos ayudarán a ver hacia dónde se desplaza el ciberespacio.

Los principios de un espacio

Los espacios tienen principios,[7] los cuales se manifiestan mediante las prácticas o las vidas que dichos espacios posibilitan o impiden en su seno. Tal como afirma Mark Stefik:

> Las barreras en el seno del ciberespacio —salas de *chat* separadas, portales de intranet, sobres digitales, y otros sistemas para limitar el acceso— se asemejan en sus efectos a las fronteras nacionales, los límites físicos y la distancia.

---

6 Para una excelente descripción, véase Jonathan Zittrain, «The Rise and Fall of Sysopdom», *Harvard Journal of Law and Technology*, núm. 10, 1997, p. 495.

7 Steven Johnson lo formula en estos términos: «En teoría, éstos son ejemplos de arquitectura y de planificación urbana, pero, en la práctica, están ligados a cuestiones más complejas: toda decisión de diseño reproduce y amplifica una serie de principios, una concepción acerca del conjunto de la sociedad donde se enmarca»; *Interface Culture: How New Technology Transforms the Way We Create and Communicate*, San Francisco, Harper, 1997, p. 44. Véase también Nelson Goodman, «How Buildings Mean» en Nelson Goodman y Catherine Z. Elgin (eds.), *Reconceptions in Philosophy and Other Arts and Sciences*, Londres, Routledge, 1988, pp. 31–48. El mismo planteamiento se aplica a las cosas, además de a los espacios. Véase Langdon Winner, «Do Artifacts Have Politics?», en *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, Chicago, University of Chicago Press, 1986, pp. 19–39 [ed. cast.: *La ballena y el reactor: una búsqueda de los límites en la era de la alta tecnología*, trad. por Elizabeth Casals Bufano, Barcelona, Gedisa, 1987]. Ahora bien, afirmar que un espacio o una cosa posee principios no equivale a decir que esto determina un resultado concreto. Hay muchas otras influencias e instancias.

> La programación determina quiénes pueden acceder dónde y qué objetos digitales pueden interactuar con qué otros objetos digitales. El modo en que dicha programación regula las interacciones humanas —modulando, así, el cambio—depende de las decisiones que se tomen.[8]

Estas decisiones suponen que espacios constituidos de forma diferente posibilitan o impiden actividades distintas en su seno. Ésta es la primera idea que deseo dejar clara. Veamos un ejemplo.

En los inicios de Internet, la comunicación se basaba en el texto. Medios tales como los grupos de noticias de USENET, *Internet Relay Chat* y el correo electrónico limitaban los intercambios al ámbito meramente textual —a palabras tecleadas por una persona (o eso se pensaba).

La razón de esta limitación resulta bastante obvia: en los inicios de Internet, el ancho de banda era muy reducido. En un entorno donde la mayoría de los usuarios estaban conectados a 1.200 baudios, y eso con suerte, los gráficos y el flujo de video en directo habrían requerido un tiempo insoportablemente largo para descargarse, si es que llegaban a hacerlo. Lo que se necesitaba era un modo de comunicación eficaz —y el texto es uno de los más eficaces.[9]

La mayoría considera este hecho de la Red primitiva como una limitación, y, en teoría, lo era. No obstante, esta descripción técnica no agota su descripción normativa como una arquitectura que posibilitaba una cierta forma de vida. Desde esta perspectiva, las limitaciones pueden pasar a ser atributos, los cuales posibilitan ciertas actividades e impiden otras. Y esta limitación en concreto favorecía a ciertos grupos de personas que salen perjudicados en la vida del espacio real.

Reflexionemos acerca de tres de estos grupos —las personas ciegas, sordas y las «feas». En el espacio real, estas personas se enfrentan a una extraordinaria variedad de impedimentos a su capacidad comunicativa. En el espacio real, las personas ciegas se enfrentan constantemente con arquitecturas

---

8 Mark Stefik, *The Internet Edge*, *op. cit.*, pp. 14–15.

9 Cfr. Godwin, *Cyber Rights: Defending Free Speech in the Digital Age*, Nueva York, Times Books, 1998, p. 42: «Si nos encontramos con una persona cara a cara, ante nuestros ojos se revelan incontables cosas sobre las cuales la otra persona no ejerce un control consciente —su color de pelo, por ejemplo, o su expresión facial. Pero cuando leemos el mensaje en código ASCII que alguien envía, todo lo que vemos es producto de la mente de esa persona»; véase también *ibidem*, p. 44.

que se presupone que pueden ver y han de esforzarse enormemente en recordarlas y actualizarlas de modo que dicha presunción no sea totalmente excluyente. Por su parte, las personas sordas se enfrentan, en el espacio real, con arquitecturas que presumen que pueden oír, debiendo también hacer esfuerzos para adaptarse. Finalmente, en el espacio real (pensemos en un bar o en un club social), las personas «feas» se enfrentan con arquitecturas de normas sociales que convierten su apariencia en un barrera para una cierta clase de intimidad, y padecen enormes sufrimientos para ajustarse a dichas arquitecturas.

Así pues, en el espacio real estos tres grupos se enfrentan con arquitecturas que les perjudican con respecto a «los demás», cosa que no les sucedía con el diseño original del ciberespacio.

Las personas invidentes podían implementar fácilmente programas que les leyeran los textos (por definición, legibles mediante máquinas) y responder mediante el teclado, de modo que el resto de la gente en el ciberespacio no tenía forma de saber que la persona que escribía el mensaje era ciega a menos que ésta lo revelara. En el ciberespacio, las personas ciegas eran iguales a las que ven.

Lo mismo ocurría con las personas sordas, que no necesitaban oír nada en la Internet original. Por primera vez, muchas personas sordas podían mantener conversaciones e intercambios en los que el rasgo más importante no era su sordera. En el ciberespacio, las personas sordas eran iguales a las que oyen.

Y lo mismo ocurría con las personas «feas». Puesto que la apariencia no se transmitía con cada intercambio, las personas poco atractivas físicamente podían mantener conversaciones íntimas con otras personas que no les definían automáticamente por su apariencia. Así, podían ligar o jugar o practicar sexo virtual (en un sentido extremadamente subestimado) sin ninguna cortapisa. Esta primera versión de la Red convertía a estas personas en iguales a «los guapos». En una sala de *chat* virtual, no sirve de mucho tener unos ojos sensacionales, una sonrisa arrebatadora o unos bíceps impresionantes. Lo que cuenta allí es el ingenio, el compromiso y la elocuencia.

La arquitectura de este ciberespacio original proporcionó a estos grupos algo de lo que carecían en el espacio real. De manera más amplia, alteró la combinación de beneficios y perjuicios que las personas debían afrontar —favoreciendo a las personas cultivadas y perjudicando a las atractivas en comparación al espacio real. Y fueron las arquitecturas las que produjeron estas ventajas y estos inconvenientes.

He contado esta historia como si los cambios sólo afectaran a aquéllos que en el espacio real presentan alguna «discapacidad». Ahora bien, el concepto de «discapacidad» es, por supuesto, relativo,[10] por lo que resulta más preciso afirmar que el espacio altera el significado del concepto de «discapacidad». Una amiga mía —una mujer de una belleza y fuerza imponentes, casada y con una vida exitosa— me describió la razón por la que se pasaba horas y horas en foros de Internet sobre política, discutiendo con otras personas acerca de los más variados asuntos públicos:

> Tú no puedes comprender lo que supone ser como yo. Toda tu vida has vivido en un mundo donde tus palabras son tomadas por lo que significan, donde lo que dices es entendido según lo que quieres decir. Antes de esto, yo nunca encontré un espacio donde se atendiera a mis palabras por lo que significaban. Antes, mis palabras eran siempre las de «esta nena», las de la «esposa» o las de la «madre». Nunca pude hablar como yo misma, pero aquí yo soy lo que yo digo.

Claramente, el espacio está *capacitándola*, por más que uno no habría afirmado que en el espacio real tenía ninguna «discapacidad».[11]

Con el paso del tiempo y a medida que el ancho de banda se fue expandiendo, esta arquitectura cambió y con ella, la combinación de beneficios y perjuicios. Cuando los gráficos llegaron a la Red de la mano de la *World Wide Web*, las personas ciegas volvieron a ser «ciegas» de nuevo; a medida que se incorporaron a los espacios virtuales archivos de sonido o de voz, las personas sordas han vuelto a ser «sordas» de nuevo; y a medida que los *chats* han comenzado a segregarse en salas donde los usuarios se ven unos a otros

---

10 Véase Martha Minow, *Making All the Difference: Inclusion, Exclusion, and American Law*, Ithaca (NY), Cornell University Press, 1990, pp. 79–97.

11 Véase Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus, Marketplace, and the Clipper Chip*, New Haven, Yale University Press, 1997, pp. 12–16. Gurak señala que «los seudónimos, por ejemplo, pueden usarse para enmascarar el nombre de un hablante, de modo que a menudo es el *ethos* de los textos y no el carácter del hablante, el que convence o no a los demás» [de esta autora, en castellano y relacionado: «Las buenas perspectivas y el peligro de la actuación social en el ciberespacio. El *ethos*, la oratoria y las protestas sobre MarketPlace y Clipper chip» en Smith y Kollock (eds.), *Comunidades en el ciberespacio, op. cit.*]. Cfr. Lori Kendall, «MUDder? I Hardly Know 'Er!: Adventures of a Feminist MUDder», en Lynn Cherny y Elizabeth Reba Weise (eds.), *Wired Women: Gender and New Realities in Cyberspace*, Seattle, Seal Press, 1996, pp. 207–233. Godwin describe otra posibilidad, en un momento en el que desaparece el canal de código ASCII de la Red: «Entonces acaso el mundo de comunicaciones mediante ASCII se convierta en una reserva para los intercambios nerviosos de maniacos del texto tenso… como yo»; *Cyber Rights*, *op. cit.*, p. 45.

mediante el uso de videocámaras, y otras donde sólo se maneja texto, las personas poco atractivas para la cámara han vuelto a ser poco atractivas.[12] Al transformarse la arquitectura, también lo hacen las definiciones de quién está «discapacitado».

Con ello no estoy defendiendo que la Red no deba cambiar —aunque, por supuesto, si puede cambiar de modo que se minimice el efecto desfavorecedor del sonido y los gráficos, sin duda debería cambiar.[13] Con toda su importancia, mi argumento no tiene nada que ver con las personas con «discapacidad». Simplemente me sirvo de este ejemplo para llamar la atención sobre un vínculo —entre estas estructuras de código y el mundo que posibilita dicho código. Los códigos constituyen los ciberespacios; los espacios favorecen o perjudican a los individuos y a los grupos. Las decisiones acerca del código representan, en consecuencia, decisiones acerca de quién, qué y, lo más importante, qué formas de vida se verán favorecidas y perjudicadas.

Ciberlugares

Podemos profundizar en el argumento expuesto mediante el examen de un cierto número de «comunidades» constituidas de modos distintos y que a su vez constituyen formas diferentes de vida, prestando atención a qué hace posibles dichas diferencias.

---

12 Esto es lo que los economistas denominarían un «equilibrio separador»: «distintas clases de jugadores adoptan distintas estrategias y, de este modo, permiten a un jugador no informado inferir a partir de las acciones de un jugador a qué clase pertenece»; Douglas G. Baird, Robert H. Gertner y Randal C. Picker, *Game Theory and the Law*, Cambridge (Mass.), Harvard University Press, 1994, p. 314. William Mitchell sostiene que el retorno a la comunicación sincrónica no necesariamente supone una ventaja: «Dada la amplia implantación y la superior eficiencia que han logrado los sistemas asincrónicos de comunicación, hemos comprobado que la sincronía estricta no siempre resulta deseable; una asincronía controlada puede tener sus ventajas»; *City of Bits*, *op. cit.*, pp. 5–16.

13 Sobre la cuestión de hacer accesible la Red, véase Judy Brewer y Daniel Dardailler, «Web Accessibility Initiative (WAI)», disponible en http://www.w3.org/WAI; cfr. «Note: Facial Discrimination: Extending Handicap Law to Employment Discrimination on the Basis of Physical Appearance», *Harvard Law Review*, núm. 100, 1987, p. 2035.

America Online

America Online (AOL) es un proveedor estadounidense de servicios de Internet —«de lejos el mayor PSI del mundo»[14] con más de 12 millones de suscriptores en 1998 y 27 millones en la actualidad.[15] Ahora bien, pese a tener una población equivalente a la suma de las de Nueva York y Nueva Jersey, AOL aún se describe a sí misma como una «comunidad»; una comunidad enorme, pero comunidad a fin de cuentas.

Esta comunidad posee una constitución —no un documento escrito (aunque también cuentan con uno), sino una forma de vida que rige a quienes viven en ella. Su filosofía de base considera que es el «sentido de comunidad» el que hace que todo sea coser y cantar en este espacio. En esta línea, desde sus inicios, AOL ha hecho hincapié en permitir que la gente interactúe a través de los *chats*, de los tablones de anuncios y del correo electrónico. (A día de hoy, AOL alberga un tráfico diario de intercambio de mensajes superior al del Servicio Postal de EEUU).[16] Los anteriores proveedores, obsesionados con proporcionar contenidos o publicidad, limitaron o ignoraron las posibilidades de interacción e intercambio que ofrecía Internet. AOL, en cambio, vio que la interacción constituía el aspecto diferencial del ciberespacio, con lo que se construyó sobre la base de la creación de una comunidad, estableciendo un lugar donde la gente pudiera decir lo que quisiera.[17]

Esta interacción está regida por las reglas del lugar. Algunas de ellas son de carácter formal, otras vienen dictadas por las costumbres sociales. Entre las primeras se encuentran los términos expresos que cada miembro suscribe al registrarse en AOL. Estos términos regulan un amplio espectro de conductas en este espacio, incluida la conducta de los miembros de AOL en cualquier otro lugar de Internet.[18]

---

14 Dawn C. Nunziato, «The Death of the Public Forum in Cyberspace», *Berkeley Technology Law Journal*, núm. 20, 2005, pp. 1115, 1125.

15 Véase AOL, «About the Company: Profile», disponible en http://web.archive.org/web/19990202213639, y ahora en http://www.corp.aol.com/whoweare/history.shtml.

16 Nunziato, «The Death of the Public Forum in Cyberspace», *op. cit.*, p. 1125.

17 Véase Kara Swisher, *Aol.com: How Steve Case Beat Bill Gates, Nailed the Netheads, and Made Millions in theWar for the Web*, Nueva York, Times Business, 1998, p. 65.

18 Tal y como queda recogido en los Términos de Servicio de AOL: «Como miembro de AOL, se le exige cumplir nuestros Términos de Servicio en cualquier sitio de Internet». Algunos de los otros términos del servicio incluyen las siguientes reglas: «Lenguaje: los improperios suaves y las referencias anatómicas sin connotaciones sexuales están permitidos, pero no así el lenguaje vulgar fuerte, las referencias sexuales groseras o explícitas, la animadversión en

Estas reglas han generado cada vez más controversia. La política de AOL ha sido tachada de prácticas de «Gran Hermano». Cuando una discusión sube de tono, afloran los improperios, pero la grosería y el lenguaje ofensivo no están permitidos en la comunidad AOL. Cuando esta elimina dichas expresiones, surgen acusaciones de «censura».[19]

Mi propósito aquí, no obstante, no es criticar estas reglas de «netiqueta». AOL también tiene otras reglas que regulan a sus miembros —reglas que no figuran en contratos, sino que más bien se hallan incrustadas en las propias arquitecturas del espacio. Estas reglas suponen la parte más importante de la constitución de AOL, pero probablemente son lo último que consideraríamos al reflexionar sobre los reguladores de la conducta en el ciberespacio.

Veamos algunos ejemplos:

Para la mayor parte de la vida en AOL,[20] sus miembros podían ser hasta cinco personas distintas. Se trataba de una característica asombrosa de este espacio. Cuando alguien abría una cuenta en AOL, tenía derecho a establecer para sí hasta cinco identidades distintas, y esto mediante cinco «nombres de pantalla» diferentes que daban lugar efectivamente a cinco cuentas distintas. Algunos usuarios, por supuesto, utilizaban los cinco nombres de pantalla para dar acceso a AOL a sus familiares, pero no todos los empleaban así. Imaginémonos a una mujer soltera que abre su primera cuenta en AOL. La compañía le ofrece hasta cinco identidades que ella puede definir a su gusto —cinco personalidades diferentes que puede emplear en el ciberespacio.

---

el discurso, etc. Si usted lo detecta, de parte en *Keyword: Notify AOL*. Desnudez: en algunos lugares (no en todos) pueden aparecer fotos que contengan prendas reveladoras o desnudez limitada en un contexto científico o artístico. No se permiten los desnudos parciales o frontales. Si usted lo ve, de parte en *Keyword: Notify AOL*. Sexo/Sensualidad: hay una diferencia entre el afecto y la vulgaridad. También hay una diferencia entre una discusión dentro de unos términos adecuados acerca de los aspectos médicos o emocionales del sexo y conversaciones sexuales más soeces. Lo primero es aceptable, lo segundo, no. Por ejemplo, en una discusión acerca de los tipos de cáncer, los términos busto o testicular serían aceptables, pero las versiones coloquiales de esas palabras no serían aceptables en ningún sitio. Violencia y abuso de drogas: imágenes explícitas de seres humanos asesinados, como las que aparecen en las noticias, pueden aceptarse en ciertas áreas, pero no la sangre y las vísceras, la violencia gratuita, etc. Las discusiones acerca de cómo afrontar el abuso de drogas en áreas dedicadas a la salud están bien, pero no las discusiones o descripciones referentes al abuso de drogas ilegales que impliquen que resulta aceptable».

19 Véase Amy Harmon, «Worries About Big Brother at America Online», *New York Times*, 31 de enero de 1999, p. 1.

20 Justo cuando se estaba completando la segunda versión de este libro, AOL se transformó en un servicio *online* gratuito. El pleno alcance del cambio que ello supondrá aún no está claro, por lo que he recurrido a formas verbales en pasado.

¿Qué significa eso? Un nombre de pantalla no es más que una etiqueta que identifica a alguien cuando se conecta al sistema, sin necesidad (y a menudo sin posibilidad) de que coincida con su nombre real. Así, si la lectora escoge StrayCat como su nombre de pantalla, entonces la gente puede contactar con ella enviando un correo electrónico a «straycat@aol.com». Si la lectora está conectada a Internet, la gente puede intentar charlar con ella buscando en el sistema AOL a la usuaria StrayCat; aparecería en la pantalla de la lectora un cuadro de diálogo que le preguntaría si desea hablar con esa persona que la busca. Si la lectora entra en la sala de *chat*, se uniría a la lista de participantes bajo el nombre de «StrayCat».

Pero, ¿quién es StrayCat? He aquí una segunda dimensión de control. StrayCat no es más que quien StrayCat dice ser. La lectora puede optar por no definirse a sí misma en absoluto, y, en caso de que decida incluir una descripción propia en el directorio de miembros, ésta puede ser tan completa o incompleta, tan verdadera o falsa, tan explícita o vaga, tan sugerente o lacónica, como ella desee. Un miembro de AOL que se tropezara con StrayCat en una sala de coleccionistas de sellos podría acceder a su perfil y leer que es una mujer soltera residente en Cleveland. Lo que suceda a continuación es una incógnita.

Ahora bien, la de StrayCat no es más que una de las cinco identidades que la lectora tiene a su disposición. Digamos que hay una personalidad diferente que StrayCat desea adoptar cuando deambula por las salas de *chat*. En ese caso, la lectora puede seleccionar otro nombre de pantalla y definirlo a voluntad en el directorio. Quizá cuando StrayCat se enfrente a una discusión profunda en un grupo de noticias o en una lista política, prefiera hablar con su propio nombre, por lo que podría seleccionar un nombre de pantalla similar al suyo y definirlo de acuerdo con quien es realmente. En otros momentos puede que StrayCat prefiera pasar por hombre —practicando el travestismo virtual y todo lo que éste pudiera traer consigo—, con lo cual optará por un nombre de pantalla masculino, y así sucesivamente. La cuestión fundamental es la multiplicidad identitaria que AOL permite y la libertad que ésta entraña.

Nadie excepto StrayCat tiene por qué saber cuáles son sus nombres de pantalla. No se le exige que revele su lista completa de identidades, y nadie puede averiguar quién es (a menos que infrinja las reglas). (Tras revelar a la Marina estadounidense el nombre de uno de sus miembros para poder procesarle por ser homosexual, AOL adoptó una política de privacidad muy estricta que promete no permitir que vuelva a ocurrir una trasgresión similar).[21]

---

21 Swisher, *Aol.com*, *op. cit.*, pp. 314–315. Disponible en http://legal.web.aol.com/aol/aolpol/comguide.html.

De este modo, AOL concedía a sus usuarios un fantástico poder para emplear seudónimos que los «desarrolladores de código» del mundo real no permiten. Por supuesto, podríamos intentar vivir la misma multiplicidad identitaria en el espacio real y, siempre que no incurriéramos en incompatibilidades o incoherencias, podríamos muy a menudo salirnos con la nuestra. Por ejemplo, podríamos ser fans de los Cubs de Chicago durante el verano y amantes de la ópera durante el invierno. Ahora bien, a menos que nos cuidemos mucho de ocultar nuestra identidad, en el espacio real siempre se nos acabará asociando a *nosotros* mismos, sin que podamos definir un personaje distinto del que somos; hemos de construir nuestro personaje y, lo que es más importante (y difícil), hemos de diferenciarlo de nuestra identidad original.

Ése es el primer atributo de la constitución de AOL —un atributo constituido por medio de su código. Un segundo atributo está ligado a la expresión —lo que se puede decir y dónde puede ser dicho.

En AOL podemos decir lo que queramos, dentro de los límites de la decencia y siempre que estemos en el sitio adecuado. Ahora bien, más allá de estos límites, la libre expresión en AOL está constreñida de un modo más interesante: no mediante reglas, sino en función del carácter de la audiencia potencial. En AOL hay lugares donde la gente puede reunirse, otros adonde la gente puede acudir a leer los mensajes de otros; pero no hay un espacio donde todos puedan reunirse al mismo tiempo, ni siquiera un espacio que todos tengan que atravesar tarde o temprano. No existe un espacio público donde poder dirigirse a todos los miembros de AOL; no existe un ayuntamiento o sala de reuniones municipal donde la gente pueda expresar sus quejas y escuchar las de los demás. No existe un lugar lo suficientemente amplio como para dar cabida a una sublevación ciudadana. Los dueños de AOL, sin embargo, sí que pueden dirigirse a todos sus usuarios. Así, Steve Case, fundador de AOL, solía escribirles cartas en un estilo «informal» donde se autoproclamaba el «alcalde» de la comunidad.[22] Case abandonó la empresa en 2005 y, por lo que parece, nadie ha ocupado su vacante en la «alcaldía», si bien los dueños de AOL, y aquéllos a quienes éstos autoricen, pueden seguir enviando publicidad y correos a todos los miembros de la comunidad. En cuanto al resto de usuarios de AOL, sólo pueden dirigirse a la multitud allá donde encuentren una —y una compuesta como máximo por treinta y seis personas (doce personas más de las que se permitían cuando apareció la primera edición de este libro).

---

22 *Ibidem*, pp. 96-97.

Éste es otro atributo de la constitución del espacio de AOL, y también viene definido mediante el código. Que sólo puede haber veintitrés personas al mismo tiempo en una sala de *chat* es una decisión de los ingenieros del código. Por más razones que puedan aducir para su opción, el efecto que provoca es claro. Resulta difícil imaginar un modo de instigar a los miembros de AOL a que se lancen a la acción pública, por ejemplo, a organizar piquetes contra la política de precios de la compañía. Existen lugares adonde acudir a quejarse, pero el usuario ha de tomarse la molestia de ir él mismo, sin que exista un sitio donde los miembros puedan quejarse en masa.

El espacio real es diferente a este respecto. Buena parte de las leyes que se ocupan de la libertad de expresión están consagradas a preservar la existencia de espacios donde pueda darse el disenso —espacios que no se puedan ignorar y a los que deban enfrentarse los ciudadanos que no disienten.[23] En el espacio real hay lugares donde la gente puede congregarse, lugares donde pueden repartirse folletos. La gente tiene derecho a ocupar las aceras, las vías públicas y otros foros públicos tradicionales, y a hablar en ellos de asuntos de interés público o de aquello que le venga en gana. La Constitución del espacio real protege el derecho de los exaltados y de los excéntricos a aparecer públicamente frente a sus conciudadanos, pero no así el diseño de AOL.[24] Como escribe Dawn Nunziato:

> AOL explica en sus Directrices de Comunidad que «como cualquier ciudad, nos enorgullecemos —y nos mostramos celosos— de nuestra comunidad». Sin embargo, a diferencia de cualquier otra ciudad, AOL disfruta de plena discrecionalidad para censurar expresiones protegidas constitucionalmente en sus foros de discusión y otros espacios *online*, incluyendo «el lenguaje vulgar» (que, advierte, «no es más adecuado en Internet de lo que lo sería en la cena de Acción de Gracias»), «las conversaciones soeces sobre sexo» y las «discusiones acerca del [...] abuso de drogas ilegales que impliquen que resultan aceptables».[25]

---

23 Véase Robert C. Post, *Constitutional Domains: Democracy, Community, Management*, Cambridge (Mass.), Harvard University Press, 1995, pp. 199–267.

24 Véase *CyberPromotions, Inc. vs. America Online, Inc.*, 948 FSupp 436 EDPa 1996, donde se sostiene que, según las Constituciones de EEUU, Pensilvania o Virginia, una compañía no está amparada en el derecho a la libertad de expresión para enviar correos electrónicos no solicitados a los clientes de la competencia.

25 Nunziato, «The Death of the Public Forum in Cyberspace», *op. cit.*, p. 1121.

Todo esto no ha de llevarnos a idealizar el poder de los foros públicos del espacio real (ni tampoco a tomarla con AOL: como continúa diciendo Nunziato, «los usuarios que busquen una mayor protección de su libertad de expresión podrían recurrir a otro PSI que no sea AOL. Eso sí, en la mayoría de los otros grandes PSI encontrarán restricciones similares a la libertad de expresión»).[26] Nos hemos convertido en una sociedad tan apolítica que si efectivamente ejerciéramos nuestro derecho constitucional a la libertad de expresión, la gente nos tomaría por locos. Si nos plantáramos en la esquina de una calle y atacáramos la última propuesta tributaria que se debate en el Congreso, es probable que nuestros amigos comenzaran a preocuparse —y no precisamente por la propuesta tributaria. Se dan excepciones —determinados acontecimientos pueden enardecer la necesidad de protestar— pero, por regla general, aunque el espacio real tenga menos control sobre el código para establecer quién puede hablar dónde, dispone de un control mayor sobre lo que la gente puede decir a través de las normas sociales. Puede que, a fin de cuentas, el espacio real se parezca mucho a AOL —el espacio efectivo para el discurso público es limitado y a menudo irrelevante—, pero mi propósito aquí es identificar el atributo y dar con la instancia que está detrás de él. Y, una vez más, nos hallamos ante un atributo definido mediante el código.

Un tercer atributo de la constitución de AOL también proviene de su código: la rastreabilidad. Mientras sus miembros están en el área de contenidos exclusiva de AOL (en otras palabras, cuando no usan AOL como un portal de acceso a Internet), AOL puede (y sin duda lo hace) rastrear sus actividades y recopilar información sobre ellos. De este modo, AOL cuenta con información acerca de qué archivos descargan, qué áreas frecuentan, quiénes son sus «colegas»; datos todos ellos enormemente valiosos y que permiten a AOL ajustar su espacio a las demandas de sus clientes. Ahora bien, el hecho de disponer de esta potestad es producto de una decisión de diseño, la cual, a su vez, forma parte de la constitución de AOL —de nuevo, una parte constituida por su código. Es una decisión que confiere a algunos, no a todos, el poder de vigilar.

AOL no ejerce este poder de manera exclusiva, sino que lo comparte. Un atributo maravilloso del espacio virtual es lo que se denomina las «listas de contactos». Si agregamos a alguien a nuestra lista de contactos, cada vez que se conecte oiremos el crujido de una puerta que nos informa de su presencia. (El «colega» no tiene por qué enterarse de que es vigilado, aunque puede, si sabe, bloquear la vigilancia). Si esa persona entra en una sala de

26 *Ibidem*, p. 1122.

chat y lo «localizamos», el sistema nos indicará dónde está. Tal poder, puesto en manos de los usuarios, puede desencadenar consecuencias engorrosas. (Imagínese el lector que está en el trabajo con la lista de contactos activada, y que ve cómo su esposa se conecta a Internet, entra en una sala de *chat* y... —bueno, el lector ya me entiende). Esta capacidad de vigilar está inserta en el diseño del espacio. Los individuos pueden desactivarla, al menos para un observador individual, pero sólo si son conscientes de ella y se plantean cambiarla.

Consideremos un último atributo de la constitución de AOL, estrechamente ligado al anterior: el comercio. En AOL podemos comprar cosas. Podemos comprarlas y descargarlas, o comprarlas y pedir que nos las envíen a casa. Cuando compramos algo, lo hacemos con nuestro nombre de pantalla y, por lo tanto, AOL sabe (aunque nadie más lo sepa) quiénes somos; y no sólo eso, también sabe dónde vivimos en el espacio real y, lo más importante, el número de nuestra tarjeta de crédito y su límite.

AOL sabe quiénes somos —he aquí un atributo de su diseño. Toda nuestra conducta en AOL está bajo vigilancia; toda ella es supervisada y asociada a nosotros como usuarios. AOL promete no recopilar datos sobre nosotros individualmente, pero sí que los recopila sobre nosotros como parte de un colectivo. Y con los datos de este colectivo, y la asociación que se puede realizar entre ellos y nosotros, AOL constituye un espacio que puede vendernos mejor y de forma más eficaz.

Estos cuatro atributos distinguen el espacio de AOL de otros lugares en el ciberespacio. AOL lo tiene más fácil para identificarnos, mientras que para los demás es más difícil; AOL lo tiene más fácil para hablar cuanto desee a todos sus «ciudadanos», mientras que para los disidentes es más difícil organizarse contra los criterios de AOL sobre cómo deberían ser las cosas; AOL lo tiene más fácil para comerciar, mientras que para los individuos es más difícil esconderse. AOL constituye un mundo normativo diferente, que la compañía crea a su antojo porque controla su arquitectura. Los miembros de ese espacio se enfrentan, en cierto sentido, a un conjunto diferente de leyes naturales, promulgadas por AOL.

Insisto en que mi propósito no es criticar la creación de este mundo, o afirmar que es abusivo. Sin duda, AOL les hace a sus miembros una serie de promesas destinadas a aliviar la preocupación que despierta este control, y si el lugar se volviera opresivo, sin duda el mercado ofrecería multitud de alternativas.

Mi propósito es más bien que nos hagamos una idea de qué es lo que hace que AOL sea como es. Como hemos visto, no se trata simplemente de reglas, de costumbres o de la oferta y demanda de un público informado; se trata en gran parte de la estructura del espacio. Al entrar en AOL, nos encontramos ante un cierto tipo de universo cuya constitución viene dada por su código. Podemos resistirnos a este código —podemos resistirnos a cómo nos determina, del mismo modo que nos resistimos al frío poniéndonos un jersey—, pero no podemos cambiarlo. Carecemos del poder para cambiar el código de AOL, y carecemos de un lugar donde poder convocar a todos los miembros para que presionen a AOL para cambiar dicho código. Nuestra vida en AOL está sujeta a sus términos; si no nos gustan, hemos de buscarnos otro sitio.

Estos atributos del espacio de AOL poseen importantes implicaciones en relación a su modo de regulación. Imaginémonos que se da un problema que la compañía desea eliminar, una conducta específica que quiere evitar o al menos controlar. ¿De qué herramientas dispone para ello?

En primer lugar, están las herramientas de las que dispone todo club, fraternidad o «comunidad». AOL puede introducir leyes de obligado cumplimiento por parte de sus miembros (y ciertamente lo hace). También puede intentar estigmatizar la conducta, sirviéndose de las normas de la comunidad para colaborar en la regulación del problema; esto se le da muy bien a AOL. De forma alternativa, y en caso de que el problema derive del uso excesivo de un recurso concreto, entonces los directivos de AOL pueden jugar con su precio, bien mediante una tasa que grave su uso con el fin de reducirlo, bien mediante la introducción de un precio diferente para aquéllos que lo emplean demasiado.

Ahora bien, éstas no son las únicas herramientas de las que dispone. Si a la compañía no le agrada una determinada conducta, puede regularla cambiando su arquitectura, al menos en algunos casos. Si trata de controlar el lenguaje indecente, AOL puede diseñar rutinas que vigilen el uso del lenguaje; si se da una mezcla inapropiada entre adultos y niños, AOL puede inspeccionar quién habla con quién; si hay un virus que crea problemas porque hay gente cargando archivos infectados, AOL puede revisarlos automáticamente mediante un programa antivirus; si se detecta la existencia de acoso, hostigamiento o amenazas, puede bloquear la conexión entre dos individuos cualesquiera.

En síntesis, AOL puede solventar ciertas clases de problemas mediante un cambio del código. Dado que el universo que sus miembros conocen (mientras están conectados) viene definido por este código, AOL puede emplearlo para regular a sus miembros.

Reflexionemos un instante acerca del poder que estoy describiendo —e insisto una vez más en que no estoy criticándolo, cuestionándolo o quejándome, sino que me limito a describirlo. Mientras nos movemos a través de este espacio que define AOL —mientras entramos en un área de *chat*, mientras publicamos un mensaje en un tablón de anuncios, mientras nos incorporamos a un espacio de discusión, mientras utilizamos la mensajería instantánea con otra persona, mientras observamos o seguimos a otras personas, mientras cargamos o descargamos archivos de distintos sitios, mientras accedemos a ciertos canales y leemos ciertos artículos, o mientras escudriñamos obsesivamente un espacio en busca de fotos de un actor o de una actriz determinados—, mientras hacemos cualquiera de estas cosas, AOL está, en un sentido importante, *ahí*. Es como si el sistema nos proporcionara un traje espacial que nos enfundamos para surcar el espacio, al tiempo que, simultáneamente, vigila todos y cada uno de nuestros movimientos.

En principio, el potencial para el control es extraordinario. Imaginémonos que AOL ralentiza el tiempo de respuesta de aquel servicio que quiere desincentivar, o que conduce al internauta a través de los anuncios que quiere que vean sus clientes, o que identifica patrones de conducta que sus sistemas de vigilancia puedan observar, basándose en la idea de que la gente con un patrón X suele ser peligrosa para la gente con un patrón Y. No creo que AOL se dedique a estas actividades y no afirmo que haya nada malo en ello, pero es importante señalar que el potencial para el control en esta «comunidad» es ilimitado —no en el sentido de que AOL podría hacer la vida imposible a sus miembros (puesto que estos acabarían yéndose de allí; en cualquier caso, tal poder, por supuesto, está controlado por el mercado) sino en el sentido de que dispone de una herramienta reguladora de la que carecen otras instancias, tanto en el espacio real como en otros tipos de ciberespacio.

En principio, pues, AOL debe elegir. Cada vez que AOL decide que desea regular un cierto tipo de conducta, ha de elegir entre al menos cuatro modalidades de regulación —las leyes, las normas, los precios o la arquitectura. De entre todas ellas, la opción de la arquitectura a menudo resulta la más conveniente.

Counsel Connect

En 1992, David Johnson lanzó *Counsel Connect* (CC) como una cooperativa de abogados *online*. La idea era sencilla: proporcionar a cada suscriptor acceso al resto de suscriptores y permitirles entablar conversaciones; mediante

este acceso y estas conversaciones se crearía el valor de la comunidad. Los juristas ofrecerían y recibirían trabajo, contribuyendo con ideas al tiempo que encontraban otras en el espacio. Así surgiría una forma diferente de práctica jurídica (menos aislada, menos exclusiva y con una base más amplia).

Pensé que la idea era estupenda, por más que a muchos les pareció un disparate. Durante un tiempo, la empresa Lexis se ocupó del sistema; en 1996 fue vendido a American Lawyer Media, LP; en 1997 migró a Internet, y su andadura concluyó en 1999.[27] En su momento álgido, pudo presumir de contar con miles de suscriptores, aunque es difícil saber cuántos contribuyeron a los debates virtuales. La mayoría sencillamente observaba las discusiones de otros, quizás agregándose a los tres o cuatro grupos que les interesaban especialmente y siguiendo otros cuantos de forma más general. Pero muchos hallaron sorprendente y novedosa la cultura que emergió en CC (al menos para los abogados). Como su fundador, David Johnson, lo describió: «Imagina un WELL de abogados, con una evolución, una apariencia, un mantenimiento y una adaptación propios y plenamente exclusivos».[28] Sus miembros llegaron a conocerse bien. «Inevitablemente, esto desembocó en numerosos encuentros en el mundo real [...] De aquéllos a los que asistí, siempre me quedó la impresión de haber estado en una reunión de viejos conocidos, por más que muchos de nosotros jamás nos hubiéramos encontrado antes cara a cara».[29]

El debate se organizaba por asuntos legales, los cuales se dividían a su vez por grupos de discusión, cada uno de ellos a cargo de un líder. Este líder no era un moderador, pues no poseía poder para eliminar un mensaje; su papel consistía en suscitar la conversación —en animar o provocar a los demás para que hablaran.

En su mejor momento, había unos noventa grupos de discusión en este espacio. El autor de un determinado mensaje podía eliminarlo, pero si él no lo borraba, su mensaje permanecía —al principio, en la lista de temas de discusión y, más tarde, en un archivo que podía ser consultado por cualquier miembro.

---

27 Correo electrónico de Alan Rothman a David R. Johnson (5 de febrero de 2006, incluido en el archivo con el nombre del autor): «Cuando, en junio de 1999, CC dejó de estar disponible de forma permanente en la Red, varios de sus miembros ya se habían anticipado y habían establecido dos nuevos foros en Delphi llamados Counsel Cafe y Counsel Politics. El final de CC se aproximaba y se vio en ellos una tabla de salvación virtual para la comunidad devota y cohesionada que había germinado en CC. Gracias a esto, unos 100 supervivientes de CC alcanzaron juntos la orilla de estos dos nuevos foros, que se establecieron como sitios privados pero a los que se permitía invitar a amigos».

28 *Ibidem*.

29 *Ibidem*.

Los miembros pagaban una cuota para registrarse en CC y se les proporcionaba una cuenta con su nombre real. Los mensajes utilizaban los nombres reales de los miembros, y cualquiera que se preguntara quién era alguien no tenía más que consultar un directorio. Los miembros de CC debían estar colegiados, a menos que se tratara de periodistas; el resto de personas no tenía derecho a acceder allí: en esto la comunidad era exclusiva.

Los mensajes de este espacio se asemejaban mucho a los publicados en un grupo de noticias de USENET. Cualquiera podía abrir un hilo de discusión, y las respuestas a él se añadirían a continuación. Dado que los mensajes no se borraban del sistema, cualquiera podía fácilmente leer un hilo de cabo a rabo. Se conservaba toda la conversación, no sólo un fragmento de ella.

Estos atributos del espacio CC obviamente fueron diseñados; los arquitectos optaron por habilitar determinados atributos y no otros. Podemos enumerar aquí algunas consecuencias de dichas opciones.

En primer lugar, estaba la consecuencia de exigir que todos los miembros emplearan su nombre real. De este modo, era más probable que pensaran antes de hablar y que se aseguraran de tener razón antes de afirmar algo tajantemente. Los miembros estaban condicionados por la comunidad, que juzgaría lo que se afirmaba sin que nadie pudiera rehuir ser asociado con lo que decía. La responsabilidad era una consecuencia de esta arquitectura, pero también lo era una cierta inhibición. ¿De verdad desea el socio de un bufete de abogados prestigioso hacer una pregunta que pondrá en evidencia su ignorancia acerca de un ámbito legal específico? Dado que los nombres no pueden cambiarse para proteger al ignorante, a menudo se optará simplemente por mantener la boca cerrada.

En segundo lugar, estaba la consecuencia de obligar a organizar las discusiones en hilos. Los mensajes se mantenían juntos; se formulaba una pregunta y con ella arrancaba el debate. Si alguien quería participar en él, primero tenía que leer los otros mensajes antes de responder. Por supuesto, esto no era un requisito técnico (siempre había la opción de no cumplirlo), pero si no se leía todo el hilo, ese alguien podía acabar repitiendo lo que otra persona había comentado antes, revelando así que estaba hablando sin escuchar a los demás. Una vez más, el uso de nombres reales liga la conducta de los miembros a las normas de la comunidad.

En tercer lugar, estaba la consecuencia relacionada con la reputación: en este espacio la reputación se construía sobre la base de la clase de consejos que se proporcionaba. La reputación de una persona sobrevivía a cualquier

mensaje concreto y, por supuesto, se veía afectada por cualquier mensaje posterior. Estos mensajes quedaban archivados y disponibles para su consulta, por lo que si alguien afirmaba algo acerca del asunto X, y luego se contradecía, su coherencia quedaría puesta en duda.

En cuarto lugar, estaba la consecuencia de asociar una determinada reputación a un nombre real en el seno de una comunidad real de profesionales. El mal comportamiento en CC trascendía fuera del espacio virtual. Por lo tanto, CC se benefició de esa comunidad profesional —se benefició de las normas de una comunidad particular. Estas normas podrían haber respaldado un comportamiento relativamente productivo dentro de la comunidad —es decir, más productivo que el comportamiento de un grupo cuyos miembros fuesen fundamentalmente distintos; y, asimismo, podrían haber respaldado la sanción a quienes se desviaran de la conducta apropiada. De esta manera, CC se benefició de las sanciones de una comunidad para controlar la conducta inadecuada, mientras que AOL tenía que confiar en su propia política de contenido para asegurarse de que la gente no se desviara del tema en cuestión.

Podemos describir de dos maneras diferentes el mundo que construyeron estos atributos de CC, del mismo modo que describimos de dos formas diferentes el mundo al que daba lugar la arquitectura de AOL. Una es la vida que posibilitaron los atributos de CC —sumamente dialógica y comprometida, aunque vigilada y con consecuencias. La otra es la regulabilidad que tiene en sus manos el responsable de la vida que se desarrolla en CC. Y aquí podemos ver una diferencia significativa entre este espacio y AOL.

CC podría haber usado las normas de una comunidad para regular de forma más efectiva de lo que AOL puede hacerlo. CC se benefició de las normas de la comunidad legal; sabía que cualquier mala conducta sería sancionada por dicha comunidad. Había, por supuesto, un rango menor de «conductas» posibles que en AOL (en CC podían hacerse menos cosas), pero como quiera que sea, la conducta en CC era regulada significativamente mediante las reputaciones de sus miembros y las consecuencias de usar sus nombres reales.

Todas estas diferencias tuvieron un efecto en la capacidad de CC para regular a sus miembros, facilitando una regulación mediante modalidades distintas del código. De este modo, y por medio de las normas, la conducta en CC se hizo más regulable que la que se daba en AOL. Puede que CC dispusiera de un menor grado de control que AOL (al fin y al cabo, sus normas de control eran las de la comunidad legal), pero también sufría menos las

cargas que conlleva la regulación de la conducta de sus miembros. Limitar el acceso, hacer pública la conducta de los suscriptores y vincularlos a sus nombres reales —he aquí las herramientas de autorregulación en este espacio virtual.

Con todo, CC se asemeja a AOL en algo fundamental: ninguna de las dos comunidades es democrática. En ambas, la dirección controla qué ocurrirá en el espacio —de nuevo, no sin restricciones, ya que el mercado constituye una restricción importante—, sin que en ninguna de ellas «la gente» tenga el poder para controlar lo que allí sucede. Acaso en CC, y de forma indirecta, existiera algo más de control democrático que en AOL, ya que en la primera eran las normas de «la gente» las que regulaban la conducta. En cualquier caso, estas normas no se podían usar directamente contra CC. Las decisiones de los administradores de CC y AOL podían haberse visto afectadas por las fuerzas del mercado (los individuos pueden abandonar las comunidades, la competencia puede robarles a sus clientes). Pero ninguna votación decide el destino de AOL, y tampoco el de CC.

Ése no es el caso del próximo ciberlugar; al menos, ya no.

LambdaMOO

LambdaMOO es una realidad virtual basada en texto. Personas de todo el mundo (hoy cerca de 6.000) se conectan a este espacio e interactúan de las maneras que éste permite. La realidad es fruto de esta interacción. Los individuos pueden participar en la construcción de esta realidad —a veces durante más de ochenta horas a la semana. Para algunos esta interacción representa el contacto humano más prolongado de toda su vida; para muchos se trata de una clase de interacción que no tiene parangón con ninguna otra cosa que hayan conocido.

Por lo general, la gente aquí se limita a hablar. Ahora bien, la gente no habla como si estuviera en una sala de *chat* de AOL. La conversación en un MUD está al servicio de la construcción —de la construcción de un personaje y de una comunidad. Uno interactúa, en parte, mediante el habla, y lo que dice se vincula a su nombre. Este nombre y los recuerdos de lo que ha hecho viven en el espacio y, con el paso del tiempo, la gente de ese espacio llega a conocer a la persona por lo que recuerda de ella.

La vida difiere dentro de cada MUD. Elizabeth Reid describe dos «estilos» diferentes—[30] el MUD social y el MUD de aventuras o de juego. Los MUD sociales son simplemente comunidades virtuales donde la gente habla y construye personajes o elementos para el MUD. Los MUD de aventuras son juegos, con premios (virtuales) o recompensas de poder que alcanzan mediante el despliegue de habilidades para conseguir recursos o derrotar al enemigo. En ambos contextos, las comunidades sobreviven a una interacción particular, convirtiéndose en clubs virtuales, si bien con distintos objetivos. Los miembros procuran construirse una buena reputación a través de su conducta.

Simplemente con registrarse en un MOO, se consigue un personaje (aunque en *LambdaMOO* la lista de espera es de varios meses). Una vez registrado, cada cual define su personaje, al menos ciertos rasgos: nombre, sexo (también se permite no especificar el sexo) y descripción. Algunas descripciones son bastante corrientes (Johnny Manhattan es «alto y delgado, pálido como el queso en barritas, y lleva un gorro de barrio»).[31]

Julian Dibbell trasladó la historia de este espacio al mundo no virtual en un artículo aparecido en el periódico neoyorquino *Village Voice*.[32] La historia en la que se centró su artículo estaba protagonizada por un personaje llamado Mr. Bungle, que resultó pertenecer a un grupo de estudiantes de la Universidad de Nueva York que compartía esta única identidad. Bungle entró de madrugada en una habitación y encontró allí a un grupo de personajes a los que conocía bien. La historia completa no puede narrarse mejor de lo que lo hizo Dibbell, si bien para nuestra finalidad aquí bastará con exponer los hechos.[33]

Bungle tenía un poder especial. Al haber conseguido un estatus especial en el seno de la comunidad de *LambdaMOO*, tenía un poder «vudú»: podía adueñarse de las voces y las acciones de otros personajes y hacer que pareciese que estaban haciendo cosas que en realidad no hacían. Esto es lo que Bungle hizo aquella noche a un grupo compuesto por varias mujeres y al

---

30 Véase Elizabeth Reid, «Hierarchy and Power: Social Control in Cyberspace», en Marc A. Smith y Peter Kollock (eds.), *Communities in Cyberspace*, *op. cit.*, p. 109.

31 Véase Josh Quittner, «Johnny Manhattan Meets the Furry Muckers», *Wired*, marzo de 1994, p. 92, disponible en http://www.wired.com/wired/archive/2.03/muds.html

32 *Ibidem*. [El relato está recogido en «Una violación en el ciberespacio», *Revista El paseante*, núm. 27-28 (*La revolución digital y sus dilemas)*, Madrid, 1998, pp. 52-57]

33 Véase, en particular, el extraordinario libro de Dibbell, *My Tiny Life: Crime and Passion in a Virtual World*, Londres, Fourth Estate, 1998.

menos una persona de sexo ambiguo. Invocó su poder en este espacio público y tomó bajo su control sus voces. Una vez controladas, Bungle «violó» a las mujeres, violenta y sádicamente, e hizo que pareciera que disfrutaban con ello.

La «violación» fue virtual en el sentido de que el suceso sólo ocurrió en los cables. «Ningún cuerpo fue tocado», tal y como describe Dibbell:

> Cualquiera que fuera la interacción física ocurrida, ésta consistió en una amalgama de señales electrónicas enviadas desde sitios repartidos entre Nueva York y Sydney, Australia. [Bungle] inició su agresión, sin que mediara provocación alguna, a eso de las 10 de la noche, hora del Pacífico. [...] Comenzó usando su muñeco de vudú para forzar a una de las ocupantes de la habitación a que le prestase servicios sexuales de formas más o menos convencionales. Esta víctima se llamaba exu... [...] acto seguido dirigió su atención a Moondreamer [...], forzándola a mantener relaciones no deseadas con otros individuos presentes en la habitación. [...] Sus acciones se volvieron cada vez más violentas [...], llegando a obligar a Moondreamer a violarse a sí misma con una pieza de cubertería de cocina. Nadie logró pararle hasta que finalmente alguien solicitó la presencia de Iggy [...], que llegó provisto de una pistola con poderes casi mágicos, una pistola que no mataba pero que envolvía a sus objetivos en una jaula impermeable incluso para los poderes de un muñeco de vudú.[34]

La violación es una palabra complicada de usar en cualquier contexto, pero en éste de manera particular. Algunos objetarán que, pasara lo que pasara en este espacio virtual, no tiene nada que ver con una violación. Pero incluso aunque «eso» no fuera una «violación», no es posible negar que existe una relación entre ésta y lo que les ocurrió a esas mujeres. Bungle utilizó su poder en beneficio de su propio deseo sexual (y en contra del de estas mujeres); sexualizó su violencia y les denegó incluso la dignidad de expresar su protesta.

Sea como fuere, para nuestra finalidad no viene al caso la discusión sobre si lo que ocurrió constituyó realmente una violación. Lo que nos concierne es el modo en que reaccionó la comunidad. Esta comunidad estaba escandalizada por lo que había hecho Bungle, y muchos pensaban que debía hacerse algo al respecto.

---

34 *Ibidem*, pp. 13-14.

Esta comunidad de miembros de *LambdaMOO* se reunió en una sala virtual a una hora determinada para discutir qué hacer. Unos treinta miembros acudieron a la cita, en lo que constituyó la reunión más concurrida que la comunidad había conocido. Algunos opinaron que Bungle debía ser expulsado —«repudiado», esto es, asesinado a efectos del MOO. Otros estimaban que no se debía hacer nada; ciertamente Bungle era un personaje detestable, pero lo mejor que se podía hacer con los de su calaña era limitarse a ignorarles. Algunos apelaron a los administradores del espacio —sus creadores, sus dioses— para que se ocuparan de Bungle, pero éstos se negaron a intervenir: su labor, replicaron, se circunscribía a crear el mundo; a partir de ahí, eran sus miembros quienes tenían que aprender a vivir en él.

Ciertamente no existía ley alguna que regulara lo que Bungle había hecho. Ninguna ley del espacio real era aplicable a este tipo de bromas sexuales, ni tampoco ninguna regla explícita de *LambdaMOO.*[35] Esto preocupaba a muchos de los que querían hacer algo. Invocando ideales del espacio real acerca de la notificación y las garantías del proceso judicial, estas personas alegaron que Bungle no podía ser castigado por violar unas reglas que no existían en ese momento.

Al final, acabaron surgiendo dos posturas extremas. Una de ellas encarecía el aumento de la vigilancia: Bungle era un maleante y debía dársele una lección, si bien *LambdaMOO* no debía incurrir, según ellos, en responder mediante la creación de un mundo de regulación. *LambdaMOO* no necesitaba Estado, sino sólo algunos buenos vigilantes que hicieran cumplir la voluntad de la comunidad sin la intromisión permanente de una fuerza central llamada Estado. Bungle debía ser expulsado, asesinado o «repudiado» —y alguien lo haría—, pero sólo si el grupo resistía la llamada a organizarse en forma de Estado.

La otra postura extrema promovía una sola idea: democracia. Con la cooperación de los administradores, *LambdaMOO* debería establecer un procedimiento para votar leyes que regularían la manera en que la gente se comportaba en el espacio. Cualquier asunto podría someterse a votación, sin que existiera límite constitucional alguno a lo que la democracia

35 En todo caso, la sexualidad del espacio invitaba a los adolescentes a responder como tales; véase Scott Bukatman, *Terminal Identity: The Virtual Subject in Postmodern Science Fiction*, Durham (NC), Duke University Press, 1993, p. 326. En particular sobre los MOO, véase Dibbell, *My Tiny Life, op. cit.* El desafío al que se enfrentaba la comunidad era el de construir normas que evitaran estas respuestas sin destruir el sabor esencial del espacio.

podría decidir. Una decisión adoptada mediante votación sería implementada por los administradores; a partir de ese momento, tal decisión constituiría una regla.

Ambas posturas tenían sus virtudes y sus defectos. La anarquía que defendía la primera planteaba el riesgo de que cundiese el caos. Era fácil imaginarse a la comunidad volviéndose en contra de la gente sin que ésta pudiera apenas advertirlo; uno imaginaba a vigilantes rondando por el espacio sin estar sujetos a ninguna ley, «repudiando» a personas cuyos crímenes lograran impactarles y resultarles «horribles». Para aquéllos que concedían menos importancia a este sitio que al espacio real, este compromiso era tolerable, pero para otros resultaba intolerable —como había podido comprobar Bungle.

La democracia parecía la solución natural, pero muchos también se resistieron. La idea de que la política pudiera existir en *LambdaMOO* parecía mancillar el espacio. La perspectiva de tener que debatir las ideas y, a continuación, votarlas suponía un nuevo lastre para el espacio. Así, si bien era cierto que las reglas serían conocidas y que podría regularse la conducta, todo eso comenzaba a asemejarse a trabajar, lo cual le restaba al espacio algo de la diversión que debía tener.

Al final acabaron sucediendo ambas cosas. El debate languideció tras casi tres horas de discusión de la que no se sacó nada en claro, y se llegó a una solución de compromiso, que Dibbell describe así:

> Fue más o menos en este punto del debate cuando Tom Traceback tomó su decisión. Tom Traceback era un administrador, un tipo taciturno que se había pasado toda la tarde absorto en sus pensamientos. Pese a no haber hablado mucho, dejaba entrever que se tomaba muy en serio el crimen cometido contra exu y Moondreamer, y que no sentía compasión alguna hacia el personaje que lo había cometido. Eso sí, había dejado igualmente claro que se tomaba muy en serio la eliminación de un jugador, y que, además, no tenía ningún deseo de volver a los días en que los administradores intervenían. Por consiguiente, debió de resultarle difícil reconciliar los impulsos contradictorios que se agitaban en su interior en ese momento. De hecho, probablemente le resultara imposible, ya que [...] por mucho que hubiera querido ser un instrumento de la voluntad colectiva del MOO, seguramente se percató de que en esas circunstancias debía, en definitiva, optar entre actuar en solitario o no actuar en absoluto.
>
> Así que TomTraceback actuó solo.

> Les dijo a los pocos jugadores que aún permanecían en la habitación que debía irse, y se marchó. Faltaba un minuto o dos para las 10 de la noche. Lo hizo en silencio y en privado; para averiguar el qué, bastaba con teclear el comando *@who*, que daba a conocer la ubicación actual de un jugador y cuándo se había conectado. Cualquiera que, poco después de la salida de Tom Traceback de la sala, hubiera tecleado dicho comando en busca de Mr. Bungle, se habría encontrado con una respuesta inesperada de la base de datos.
>
> «El nombre de Mr. Bungle», habría respondido, «no corresponde a ningún jugador».
>
> La fecha en que ocurrió esto fue el día de los Inocentes (*April Fool´s Day*), pero aquello no era ninguna broma: verdaderamente Mr. Bungle había muerto y desaparecido.[36]

Cuando los administradores se dieron cuenta, se fueron al otro extremo. Sin mediar una decisión formal de los ciudadanos, los administradores instauraron una democracia. A partir del 1 de mayo de 1997,[37] cualquier asunto podía decidirse mediante votación, y cualquier propuesta que recibiera, como mínimo, el doble de votos a favor que en contra pasaría a tener rango de ley.[38] Muchos se preguntaron si aquello suponía un avance o no.

Esta historia nos da mucho que pensar, incluso en mi versión enormemente abreviada.[39] No obstante, deseo centrarme en el sentido de pérdida que acompañaba la decisión de los administradores. Hay un cierto romanticismo asociado a la idea de establecer una democracia —anuncios de Kodak con berlineses llorando mientras cae el Muro y toda la parafernalia. El romanticismo radica en la idea del autogobierno y del establecimiento de estructuras que lo permitan. Pero el paso a la democracia de *LambdaMOO*, mediante la implantación de estructuras democráticas, no sólo suponía un logro, sino también un fracaso. Así, podríamos decir que el espacio había fracasado en su autorregulación, en la generación entre su población de principios que bastaran para evitar precisamente la clase de fechoría que había cometido Bungle. El debate señaló la transición de una clase de espacio a otro, de un espacio autorregulado a uno regulado por sí mismo.

---

36 Dibbell, *My Tiny Life*, *op. cit.*, pp. 24–25.

37 Véase Rebecca Spainhower, *«Virtually Inevitable»: Real Problems in Virtual Communities,* Evanston (Illinois), Northwestern University Press, 1994, disponible en http://web.archive.org/web/19990202105057re_/vesta.physics.ucla.edu/~smolin/lambda/laws_and_history/ballothistory.

38 *Ibidem*.

39 Para un valioso relato acerca de la democracia y su funcionamiento, así como acerca de las implicaciones de la autorregulación en un MUD, véase Jennifer Mnookin, «Virtual(ly) Law: The Emergence of Law on LambdaMOO», *Journal of Computer-Mediated Communication*, núm. 2, 1996, p. 1.

Puede parecer extraño que exista un lugar donde la emergencia de la democracia abatiese a la gente, pero este tipo de reacción no deja de ser habitual en los ciberlugares. Katie Hafner y Matthew Lyon cuentan una historia sobre la aparición en UNIX de un «trasto» llamado el comando FINGER, que permitía a los usuarios conocer cuándo fue la última vez que otro usuario había utilizado el ordenador y si había leído su correo electrónico. Algunos pensaron (lo cual no me sorprende) que este comando era una especie de invasión de la privacidad. ¿A quién le importa cuándo fue la última vez que utilicé mi ordenador y por qué deberían averiguar si he leído mi correo?

Un programador de la Carnegie Mellon University, Ivor Durham, modificó el comando para permitir al usuario eludir este *dedo* espía. ¿Cuál fue el resultado? «Durham fue vituperado sin piedad mediante *flaming*. Le llamaron de todo, desde pusilánime a irresponsable social, pasando por político de pacotilla y cosas peores —y no por proteger la privacidad, sino por andar trastocando la apertura de la red».[40]

Los principios del mundo UNIX eran diferentes. Se trataba de principios integrados en el código de UNIX, por lo que cambiar el código suponía cambiar estos principios, algo contra lo que lucharon los miembros de esa comunidad.

Lo mismo ocurrió con los cambios en *LambdaMOO*. Antes de instaurar las votaciones, esa comunidad se regulaba mediante normas. Estas regulaciones de las estructuras sociales se sustentaban en la constante acción política de los ciudadanos individuales, por lo que constituían las regulaciones de una comunidad. Con el ascenso de la democracia sobrevino la decadencia de esta comunidad y, aunque las normas sin duda sobrevivieron en el nuevo contexto, su estatus cambió para siempre. Antes de la democracia, una disputa acerca de qué normas deberían prevalecer sólo podía resolverse mediante consenso —esto es, mediante ciertos puntos de vista que predominan de una manera descentralizada.

Este pequeño extraño mundo ha quedado más idealizado de lo que pretendía. No quiero sugerir que *LambdaMOO* antes de la democracia fuese necesariamente mejor que el que surgió después. Sólo quiero señalar una modificación específica. Como en Councel Connect, y no en American

---

40 Hafner y Lyon, *Where Wizards Stay Up Late*, *op. cit.*, p. 216. El término inglés *flaming* describe un correo electrónico o cualquier otra comunicación electrónica que expresa hostilidad exagerada; véase Gurak, *Persuasion and Privacy in Cyberspace*, *op. cit.*, p. 88.

Online, en *LambdaMOO* las normas regulan; pero, a diferencia de CC, en *LambdaMOO* los miembros detentan el control sobre la reestructuración de las normas.

Este control cambia las cosas. Las normas se vuelven diferentes cuando las votaciones pueden anularlas, y el código se vuelve distinto cuando las votaciones pueden ordenar que los administradores cambien el mundo. Estos cambios marcan un movimiento de un tipo de espacio normativo a otro, de un tipo de regulación a otra.

En los tres ciberlugares que hemos examinado, el código es un regulador, pero existen importantes diferencias entre ellos. En CC y en *LambdaMOO*, las normas tienen una relevancia de la que carecen en AOL; la democracia tiene una relevancia en *LambdaMOO* que no tiene en CC o en AOL. Y la vigilancia tiene una relevancia en AOL que no tiene en *LambdaMOO* o en CC (ya que ninguna de estas dos comunidades emplea datos personales con propósitos comerciales, ya sean internos o externos a la organización). El código constituye estas tres comunidades; tal como afirma Jennifer Mnookin respecto a *LambdaMOO*, «la política se lleva a cabo a través de la tecnología».[41] Las diferencias en el código las constituyen de modos diferentes, y algunos códigos contribuyan más que otros a que las comunidades sean más tupidas. Y allá donde hay una comunidad tupida, las normas pueden regular.

El siguiente espacio de este estudio también está constituido mediante el código, si bien en este caso la «dirección» tiene menos capacidad para cambiar su arquitectura básica. Dicho código es código de red —un protocolo de Internet que un usuario aislado no puede cambiar fácilmente. Al menos a mí me resultó complicado.

.law.cyber

Se llamaba IBEX y nadie llegó a saber quién era. Es probable que yo hubiera podido averiguarlo —disponía de los datos para seguirle el rastro—, pero después de lo que hizo, preferí no saberlo. Seguramente era uno de los estudiantes del primer curso que impartí sobre ciberespacio, y de buena gana lo

41 Mnookin, «Virtual(ly) Law», *op. cit.*, p. 14.

habría suspendido —tanto me enfadaron sus acciones. Mi curso se titulaba «El Derecho del Ciberespacio» y su primera versión la impartí en la Universidad de Yale.

Digo primera versión porque tuve la extraordinaria oportunidad de impartir ese curso en tres excelentes facultades de derecho de EEUU —primero en la de la Universidad de Yale, luego en la de Chicago y, por último, en la de Harvard. Se trata de tres lugares muy diferentes, con tres tipos de alumnado igualmente distintos. Sin embargo, mantuve una parte del curso idéntica en las tres facultades y cada año creaba un «grupo de noticias» asociado al curso —un boletín electrónico donde los estudiantes pudieran publicar mensajes sobre las cuestiones que surgían en el curso, o sobre cualquier otro asunto. Estos mensajes originaban conversaciones —hilos de discusión, compuestos de mensajes correlativos, donde se debatía o se cuestionaba lo que se había afirmado en el mensaje anterior.

Estos grupos de noticias constituían lo que los filósofos denominarían «comunidades dialógicas». Eran espacios propicios para el debate, pero con el añadido de que lo que alguien decía se archivaba para que los demás pudieran consultarlo, como ocurría en CC. He aquí el componente dialógico. La comunidad se conformaba con el paso del tiempo, a medida que la gente se iba conociendo —tanto en este espacio como en el espacio real. Un año los alumnos de mi curso celebraron una fiesta junto con otros alumnos que no estaban matriculados (pero que habían estado siguiendo el transcurso de los debates en .law.cyber); otro año, aquéllos invitaron a éstos a asistir a una de mis clases. Sea como fuere, lo que quedó claro es que, al cabo de tres años impartiendo el curso en tres facultades distintas, habían surgido tres comunidades, cada una nacida en una fecha concreta y mantenida con vida durante al menos un par de meses.

La historia que narro a continuación proviene de la comunidad de Yale. La Facultad de Derecho de esta universidad tiene sus peculiaridades, en un sentido positivo. Es una facultad pequeña que rebosa de gente extremadamente brillante, mucha de la cual no desea realmente acabar dedicándose al Derecho. Se organiza a sí misma como una comunidad donde todos, del Decano para abajo (si bien esta expresión no encaja con el estilo «Yale») se afanan por fomentar y mantener este sentido de comunidad entre el alumnado. Y, en gran medida, funciona —no en el sentido de que allí reine una paz perpetua, sino en el sentido de que, esté donde esté, la gente es consciente de este sentido de comunidad. Algunos lo abrazan y otros se resisten, pero ambas actitudes indican que dicho sentido de comunidad existe. Uno no se resiste a la comunidad de pasajeros de un autobús interurbano.

Una de las peculiaridades extraordinarias de la Facultad de Derecho de Yale es la presencia en ella de «El Muro». El Muro es un lugar donde la gente puede dejar sus comentarios sobre lo que le venga en gana. Allí se puede colocar desde un escrito sobre los derechos de los gays en la Universidad de Yale hasta una protesta sobre el trato que ésta dispensa a los trabajadores sindicados; también mensajes políticos u opiniones sobre Derecho. Cada mensaje posibilita que se le añadan otros —bien garabateados en la misma hoja de papel, bien anexados debajo.

El Muro constituye un símbolo extraordinario para cualquier visitante, emplazado como está justo en medio de la Facultad. En el centro de una estructura neogótica se halla un espacio de piedra con decenas de papeles colocados abigarradamente. Alrededor, se encuentran estudiantes que pasan por allí y se detienen a leer lo que otros han escrito. El Muro es a la Universidad de Yale lo que el *Speakers' Corner* es a Hyde Park,[42] si bien en este caso no hay oradores sino escritores, y la escritura es algo sustantivo. En El Muro, la retórica sirve de bien poco; para granjearse respeto, uno ha de escribir algo sustancioso.

Una regla, no obstante, gobierna este espacio. Todos los mensajes han de llevar firma; en caso contrario, son retirados. Originalmente, sin duda, la regla implicaba que el mensaje debía ir firmado por su autor. Pero como estamos hablando de Yale, donde no puede existir ninguna regla que no suscite millares de preguntas, ha surgido la costumbre de permitir la publicación de mensajes anónimos bajo la firma de alguien que no es su autor (con la coletilla «Firmado, pero no escrito, por X»). Esa firma le concede al anónimo el pedigrí que necesita para sobrevivir en el Muro.

Las razones de esta regla son claras, al igual que los problemas que genera. Pongamos que el lector desea criticar una decisión que ha tomado el Decano. Éste, por más complaciente que sea, es una persona poderosa, por lo que es posible que el lector prefiera publicar su crítica sin que aparezca su nombre debajo. O pongamos que el lector es un estudiante cuyas ideas políticas le convierten en un inadaptado. Exponerlas en el Muro con su firma puede suponer el desprecio de sus compañeros. La libertad de expresión no equivale a una expresión libre de consecuencias, y muchas expresiones traen como consecuencia el desprecio, la vergüenza o el ostracismo.

---

42 El *Speakers´ Corner* (literalmente, la «Esquina de los Oradores») es una zona situada en el extremo noreste del parque londinense de Hyde Park (aunque también se denomina así a zonas similares de otros parques de Londres y de distintas ciudades) que es célebre por albergar discursos públicos y debates, además de protestas y manifestaciones, ya desde la segunda mitad del siglo XIX. [N. del E.]

El anonimato constituye, pues, un modo de sortear este dilema. Con él podemos decir lo que queramos sin temor. En algunos casos, y para algunas personas, tiene sentido apelar al derecho de expresarse anónimamente.

Con todo, es posible que una comunidad quiera resistirse a este derecho. Del mismo modo que el anonimato puede dotar a alguien de la fuerza para manifestar una opinión impopular, también puede servirle de escudo para verter juicios irresponsables, difamatorios o hirientes. Puede que el lector quiera cuestionar la política del Decano o puede que quiera acusar en falso a un compañero de copiarse en el examen. Ambas declaraciones se benefician del anonimato, pero la comunidad posee buenas razones para oponerse a las del segundo tipo.

Que yo sepa, IBEX nunca escribió nada en El Muro. En lugar de ello, escogió el grupo de noticias asociado a mi curso, cuyo diseño estaba abierto a las contribuciones de cualquier alumno de Yale. A diferencia del Muro, sin embargo, la tecnología de este grupo de noticias permitía a sus usuarios emplear un nombre cualquiera. «IBEX», por supuesto, era un seudónimo. Por lo que respecta al Muro, recurrir a un seudónimo equivale al anonimato —ya que el que escribe sigue sin revelar su nombre real—, pero esto no es así en un grupo de noticias. Con el paso del tiempo, se puede llegar a conocer a quien hay detrás de un seudónimo. Aquel año, además de IBEX, teníamos en clase a SpeedRacer, MadMacs, CliffClaven, Aliens, blah y Christopher Robbin. Y por más que los miembros de la clase pudieran llegar a saber quiénes eran estos participantes (todos sabíamos quién era MadMacs, pero sólo unos cuantos conocíamos la identidad de SpeedRacer), cada seudónimo representaba a un personaje.

El personaje de IBEX era malo; eso quedó meridianamente claro desde el inicio. Antes de que él apareciese, la vida en este espacio florecía. Al principio, la gente se mostraba tímida pero siempre correcta; las almas osadas lanzaban una idea o un chiste, y de ahí surgía una conversación que no solía prolongarse demasiado. Al cabo de dos semanas, las conversaciones ganaron intensidad y comenzó a fluir el intercambio de ideas. Algunos formulaban preguntas y otros las respondían. Por más que se les trabase la lengua, los participantes estaban, lentamente, empezando a hablar.

Ciertos rasgos característicos de su forma de hablar quedaron patentes de inmediato. En primer lugar, las mujeres intervenían en el grupo de noticias más de lo que lo hacían en clase; acaso no de manera estadísticamente

significativa, pero más, al fin y al cabo.[43] En segundo lugar, dentro del grupo surgió rápidamente una diferenciación entre quienes prestaban su ayuda a los demás y quienes la recibían. En poco tiempo se creó una clase paralela en Internet —una clase real que se identificaba a sí misma como tal y que se expresaba como clase del modo soñado por cualquier profesor en el espacio real, de una manera que yo nunca había visto.

No sabría decir por qué ocurrió esto. Acaso Una Smith se erigió como catalizadora de todo aquello. Como dije más arriba, impartí este curso en tres ocasiones, y siempre (sin intervención alguna por mi parte) aparecía en el grupo de noticias alguien como Una Smith. En Yale era una persona real pero después la consideré como un tipo de persona. Siempre se trataba de una mujer que no pertenecía a la clase, que poseía conocimientos muy amplios sobre la Red y USENET y que rondaba por mi clase (virtual) diciéndoles a los demás cómo debían comportarse. Cuando alguien transgredía una norma de la Red, Una le corregía, lo cual no solía sentar muy bien entre los participantes (al fin y al cabo, eran estudiantes de Derecho), que enseguida cerraban filas en torno a ese alguien y retaban a Una a defender sus reglas. Como no podía ser de otra forma, ella demostraba estar curtida en estas lides y usualmente hallaba una respuesta que respaldaba las reglas que había dictado. Este intercambio pronto se convirtió en un centro de atención para la clase. Una Smith había provocado el enfado de la clase y, de resultas, ésta ganó cohesión.

Tras un mes y medio de curso, el grupo de noticias alcanzó su punto álgido; la cosa no podía ir mejor. Recuerdo bien el momento en que me percaté. A primera hora de una tarde de primavera me fijé en que alguien había publicado la primera línea de un poema; hacia el final del día, y sin ninguna coordinación, la clase lo había completado. Hasta entonces, había habido ritmo en los intercambios; ahora había también rima. La cosa estaba que ardía en el grupo, y sus usuarios estaban genuinamente sorprendidos de las posibilidades de este espacio.

Fue entonces cuando apareció IBEX. Creo que fue justo después de que discutiésemos sobre el anonimato en clase, así que acaso fuera cierto su alegato posterior de haber actuado con fines pedagógicos. Sea como fuere, hizo su aparición después de una de nuestras clases —y con la única finalidad,

---

43 Uno de mis alumnos analizó este comportamiento y concluyó que la diferencia era significativa, si bien se basó en una muestra de población relativamente reducida. En un estudio más general sobre la cuestión, Gurak llega a una conclusión diferente sobre si el ciberespacio remedia la discriminación en función del sexo; *Persuasion and Privacy in Cyberspace*, *op. cit.*, pp. 104–113.

según pareció, de lanzar un ataque contra otro miembro de la clase. Y no un ataque contra sus ideas, sino contra su persona; y uno tan despiadado y tan amplio que, cuando lo leí, no acerté a saber cómo interpretarlo. ¿De verdad podía haber ocurrido aquello?

Casi inmediatamente la conversación en el grupo murió. Se interrumpió, así, sin más. Nadie se pronunció de ninguna forma, como si todos temieran que el monstruo que había entrado en nuestro espacio los escogiera como el siguiente blanco de su furia. Hasta que, finalmente, la víctima respondió, con un mensaje que evidenció cuánto le había dolido el ataque. Las palabras de IBEX habían hecho mella y ahora, enfadada y herida, la víctima contraatacaba.

Su acometida no hizo sino inspirar otra salva de crueldad, incluso más vil que la primera, que empujó a otros miembros de la clase a tomar parte. Una serie de personajes del grupo de noticias tacharon a IBEX de cobarde por ocultarse detrás de un seudónimo, y de depravado por lo que había dicho. Nada de esto afectó en lo más mínimo a IBEX, que volvía a las andadas una y otra vez, con una acritud tan extrema como implacable.

El espacio había quedado definitivamente afectado. La conversación decayó y la gente fue abandonando el grupo de noticias. Sin duda, algunos lo hicieron porque se sentían indignados ante lo que había ocurrido, pero otros simplemente no querían ser la siguiente víctima de IBEX. Mientras la gente permaneció conjurada para atacar a IBEX, el espacio logró mantenerse brevemente con vida, pero como éste seguía interviniendo una y otra vez, cada vez con más saña, la mayoría simplemente optó por abandonar el grupo. (Una vez IBEX apareció para manifestar su protesta; la semana anterior, afirmaba, no había publicado ningún mensaje, pero alguien lo había hecho haciéndose pasar por él, con lo que él, el auténtico IBEX, había sido difamado. La clase no le compadeció demasiado).

Ahora bien, todo esto no sólo afectó a la clase virtual. A medida que nos encontrábamos cara a cara semana tras semana, yo percibía el ambiente de clase cada vez más viciado. El alumnado sentía la presencia de la criatura en el aula, por más que nadie pudiera creer que se tratara de un estudiante de la Facultad de Derecho de Yale. IBEX era uno de sus compañeros de clase, camuflado tras una sonrisa o un chiste en el espacio real, despiadado en el ciberespacio. Y la mera idea de que tamaña crueldad pudiera esconderse tras una sonrisa cambió el modo en que la gente percibía las sonrisas.

Algunos denominaron esto el «efecto David Lynch», en alusión al cineasta estadounidense que retrata la podredumbre de la sociedad que se oculta justo detrás de fachadas recién pintadas. En la clase podíamos percibir la podredumbre de nuestra comunidad justo detrás de un alumnado sonriente y aplicado. Había un Jake Baker (relativamente domesticado) entre nosotros. El espacio había permitido una conducta que destruyó la comunidad —una comunidad que el propio espacio había creado. Y es que dicha comunidad se había creado, en parte, mediante la capacidad de ocultar —de ocultarse tras un seudónimo benigno; de ocultar la vacilación a la hora de escribir o de corregir lo que otros habían escrito; de ocultar las reacciones; de ocultar que no se estaba prestando atención. Este anonimato había hecho de la comunidad lo que era. Ahora bien, el mismo anonimato que creó la comunidad engendró también a IBEX, dando así al traste con ella.

Second Li(f/v)e(s)

Los cuatro ciberlugares que acabo de examinar aparecían ya en la primera edición de la presente obra, cada uno de ellos descrito prácticamente en los mismos términos. Se trata, pues, de viejas historias, y las lecciones que nos enseñan coinciden exactamente con lo que se intenta exponer en este capítulo. Con esto no pretendo sugerir que en todo este tiempo no se hayan producido progresos interesantes en los ciberespacios que ha inspirado Internet. Los últimos cinco años han sido testigos de una explosión de ciberespacios mucho más espectacular de lo que hubiera podido imaginar cuando escribí la primera versión de *El código*.

De alguna manera, estos espacios no constituyen nada realmente nuevo. Se benefician de las flamantes nuevas tecnologías que, gracias a que los ordenadores son más rápidos y la banda ancha ha aumentado de capacidad, funcionan mucho mejor que sus anteriores versiones. Con todo, el espacio MMOG que describí en el Capítulo 2 estaba inspirado en espacios reales.

Lo que sí que ha cambiado es el tamaño. Tal y como Julian Dibbell me explicaba, la cuestión es:

> ¿Importa el tamaño en este tipo de espacios? Yo creo que sí. El mundo basado en texto está naturalmente limitado en su tamaño. El límite no viene impuesto tanto por la oposición entre texto y gráfico como por la oposición entre una accesibilidad cultural limitada y otra mucho más amplia. Eso es lo que genera espacios más grandes.[44]

El resultado es «algo socialmente más rico en muchos aspectos», «y no tanto la disponibilidad particular de imágenes en 3D, que algún día también nos parecerán bastante toscas».

Los juegos de rol *online* para múltiples jugadores (los MMOG o MMORPG) se han convertido en toda una industria. Literalmente millones de personas pasan cada año cientos de horas, a veces incluso miles, en estos espacios, gastándose miles de millones de dólares en vivir estas *segundas vidas*. Por supuesto, éstas han de compaginarse con sus vidas en el espacio real. Cuando alguien juega al *World of Warcraft*, al mismo tiempo está desempeñando su rol de padre o de esposa en el espacio real. Por lo tanto, ese alguien no ha abandonado el mundo real para ir a esos otros lugares, sino que los integra en su vida del mundo real; y los últimos cinco años han visto una explosión del porcentaje de vida del mundo real que es vivida virtualmente.

Estos «juegos» pueden dividirse de un modo muy elemental en dos tipos. En el primero, la gente «juega» a un juego que otros han definido: estos son los «juegos de rol». En este sentido, *World of Warcraft* es un juego de rol en el que la gente compite para cosechar riquezas y estatus (por lo que no es tan diferente de la vida real). *Grand Theft Auto* es un juego en que la gente se entrega a una suerte de delito virtual. Todos estos juegos poseen una estructura propia, pero difieren en el grado en que la gente puede adaptarlos a sus gustos o crear sus propios personajes o escenarios. Según estas consideraciones, la inmensa mayoría de juegos *online* son juegos de rol. Un sitio dedicado a seguir la pista a estas comunidades estima que el 97 % de los juegos *online* son juegos de rol de alguna clase.[45]

El segundo tipo conlleva un grado mucho mayor de elaboración. Estos espacios generan comunidades donde la gente, como mínimo, hace vida social, además de desarrollar actividades creativas y comerciales.

---

44 Grabación de audio: entrevista con Julian Dibbell (6 de enero de 2006; incluido en el archivo del autor).

45 Página principal de MMOGCHART.com, disponible en http://mmogchart.com.

Dependiendo del juego del que se trate, la combinación de estas actividades difiere sustancialmente. En cualquier caso, todos ellos aspiran a crear un mundo virtual que inspire la aparición de una comunidad real en su seno. Estos juegos son una prolongación de los MOO que describí más arriba, pero extienden la comunidad virtual más allá del círculo de los avezados en la manipulación de textos. Y por más que sean virtuales, estos mundos son gráficamente reales.

Por supuesto, dentro de ambos tipos de MMOG existe creatividad, constituyendo las diferencias entre ellos simplemente una cuestión de grado. Y también en ambos se dan actividades comerciales. *Second Life* —que describiré más abajo— genera al mes más de «cuatro millones de dólares en transacciones interpersonales».[46] Si sumamos las cifras que se mueven en los diferentes juegos, comprobaremos que, como describe Edward Castronova, estos mundos virtuales producen un gran volumen comercial:

> El flujo comercial que genera la gente que compra y vende dinero y otros artículos virtuales (esto es, varitas mágicas, naves espaciales, armaduras) asciende a un mínimo anual de 30 millones de dólares en EEUU, y de 100 millones en todo el mundo.[47]

Aún más interesante (y chocante) resulta el cálculo de Castronova acerca del Producto Interior Bruto *per cápita* que se produce en varios mundos virtuales. *EverQuest*, por ejemplo, tiene un PIB de casi la mitad del de «la República Dominicana»;[48] y el PIB *per cápita* de *Norrath* «era prácticamente el mismo que el de Bulgaria y cuatro veces superior al de China o India».[49]

Por lo que respecta a mi finalidad aquí, no obstante, me centraré en el segundo tipo de MMOG y, en particular, en dos ejemplos de él. El primero fue un líder temprano en este espacio —*There*; el segundo constituye un éxito ascendente y extraordinario —*Second Life*.

Second Life es, según la descripción de su página web, «un mundo virtual en 3D enteramente construido y poseído por sus residentes». Un mundo en 3D en el sentido de que la experiencia allí parece tridimensional —los personajes y

46 Grabación de audio: entrevista con Philip Rosedale (13 de enero de 2006; incluido en el archivo del autor).

47 Castronova, *Synthetic Worlds*, *op. cit.*, p. 2.

48 Julian Dibbell, «Dragon Slayers or Tax Evaders?», *Legal Affairs*, enero/febrero de 2006, p. 47.

49 Castronova, *Synthetic Worlds*, *op. cit.*, p. 19.

los objetos aparentan tener tres dimensiones. Un mundo virtual en el sentido de que los objetos y las personas que lo pueblan están diseñados con ordenadores. Un mundo construido por sus residentes ya que *Second Life* se limitó a proporcionar una plataforma sobre la cual construyen sus residentes. (Y no lo hicieron entre unos cuantos. En un día cualquiera, el 15 % de residentes está editando la secuencia de comandos que hace funcionar *Second Life*.[50] En sus orígenes, esa plataforma presentaba unos bellos campos verdes y a medida que los residentes adquirieron terrenos en ese mundo, comenzaron a construir estructuras). Y un mundo poseído por sus residentes en el sentido de que aquello que construyen los residentes de *Second Life* es suyo —tanto el propio objeto «físico» (el coche, la tabla de surf o la casa) como cualquier derecho de propiedad intelectual que pueda recaer sobre lo que han construido allí.

Es esta última característica la que contrasta de modo más interesante (al menos, para mí) con el otro MMOG que he mencionado, *There*. *There* también era un mundo virtual, pero radicalmente diferente de (y con menos éxito que) *Second Life*, centrado en las franquicias corporativas —se esperaba que Sony o Nike, por ejemplo, abrieran una tienda en *There*. A la gente también se le permitía crear cosas en este mundo virtual, y cuando las vendían o las regalaban, *There* se llevaba un porcentaje de la operación. El espacio en sí mismo venía ya bastante prefabricado, pero dejaba a los residentes un margen significativo para adaptarlo a sus preferencias.

Los fundadores de *There* construyeron la retórica de este mundo basándose al menos en (lo que ellos entendían como) los ideales de EEUU. El tipo de cambio de los dólares-*There* era de 1787 por 1 —aludiendo 1787 al año en que se redactó la Constitución de EEUU. Y el por entonces Director Ejecutivo de *There* explicó en una de mis clases que los principios de la República estadounidense eran los que informaban los principios de *There*.

Esta declaración fue recibida con escepticismo entre mi alumnado, y una estudiante extraordinariamente brillante, Catherine Crump, le dio al Director Ejecutivo un pequeño vapuleo. En primer lugar, le preguntó si *There* respetaría los principios de la Primera Enmienda. «Por supuesto», respondió el Director Ejecutivo. «¿Estaría autorizada una ciudadana de *There* a colocar un cartel en su terreno?». «Por supuesto». «¿Estaría autorizada a adquirir terreno cerca de, digamos, la sede de Nike?». «Por supuesto».

50 Grabación de audio: entrevista con Philip Rosedale (16 de enero de 2006; incluido en el archivo del autor).

«¿Estaría autorizada a colocar en ese terreno un cartel que dijera "Nike emplea fábricas donde se explota a los obreros"?». «Umm. No estoy tan seguro de eso». Bonita forma de respetar la Primera Enmienda.

O, más en relación con *Second Life*, Crump continuó preguntando: «¿Quién ostenta la propiedad intelectual de los diseños que elabora un ciudadano?». «*There*». «Y ¿quién ostenta la propiedad intelectual de los diseños de Nike?». «Nike, por supuesto. ¿De qué otra forma podría ser?». «Bueno, sí que podría ser de otra forma, si *There* siguiera los principios de la Constitución de EEUU» sugirió Crump, añadiendo que «los derechos de propiedad intelectual pueden ser ostentados por "autores o inventores", no por corporaciones».

El auténtico problema de *There*, no obstante, era estructural, siendo el mismo que aqueja a cualquier economía centralizada o planificada. *There* tenía que ser construido por *There, Inc.*; y ahí radicaba su problema. Las estructuras de estos mundos virtuales son extraordinariamente complejas, y el coste de construirlas es inmenso, por lo que *There, Inc.* tenía que hacer frente a un enorme desembolso de capital para que *There* funcionase.

Second Life (como todas las nuevas naciones) trasladó ese coste de construcción a los ciudadanos, a modo de una *subcontrata*. Cuando alguien adquiere terreno en *Second Life*, recibe un campo vacío o una isla desierta. A partir de aquí, hay que comprar, construir o conseguir mediante trueque lo necesario para hacer habitable ese terreno. Existen negocios en torno a la construcción, y ésta puede exigir esfuerzos considerables, pero siempre se puede vender aquello que se construye. E, insisto, los diseños que alguien realiza le pertenecen. Actualmente, más de 100.000 personas habitan, y construyen, *Second Life*. Para ellos el juego representa realmente una «segunda vida».

Estas reglas actuales, no obstante, son producto de una evolución en la concepción de *Second Life*. En la primera versión Alfa que se hizo pública del sitio que luego se convertiría en *Second Life*, no se contemplaba la propiedad del terreno, sino que todo era público. Dicha propiedad se incorporó en la versión Beta, cuando todos los usuarios pudieron reclamar el terreno público a un determinado precio. Una vez hecho esto, el usuario decidía si los demás podían crear objetos, guiones o puntos de referencia para ese terreno. Posteriormente estas opciones se extendieron aún más.

En la versión 1.1, se agregó una profunda modificación a las leyes físicas que regían el terreno. Mientras que antes los usuarios tenían la libertad de teletransportarse a cualquier parte, ahora, para evitar el hostigamiento, los

propietarios de terreno podrían decidir si permitían o no que otros «allanaran» su propiedad —bien estableciendo por defecto si se permitía o se denegaba el acceso, bien añadiendo una lista de personas que eran libres de visitar su propiedad. Ahora bien, estas restricciones sólo se aplicaban a 15 metros por encima de la propiedad; por encima de esa altura, cualquiera tenía la libertad de atravesar la propiedad volando, por más que el propietario no quisiera permitirles el paso.

Existe un interesante paralelismo entre esta última restricción y la historia del Derecho estadounidense. Tal y como describo en *Por una cultura libre*,[51] el régimen de propiedad en la tradición legal estadounidense consideraba que el propietario de un terreno poseía el espacio que se elevaba desde el suelo «hasta una longitud indefinida hacia arriba».[52] Tal consideración desencadenó un conflicto obvio cuando aparecieron los aviones. ¿Cometía el piloto de un avión un allanamiento cuando volaba sobre el terreno de alguien?

La conciliación que el Derecho introdujo finalmente se basó en la distinción entre volar muy bajo y volar muy alto. No se cometía allanamiento si se volaba a gran altura sobre el terreno de alguien; el perjuicio venía si el vuelo se realizaba a poca altura. Así pues, el Derecho ya había llegado a una solución similar a la propuesta por *Second Life*.

Fijémonos, no obstante, en la importante diferencia existente entre una y otra regulación. En el espacio real la ley establece penas por violar la regla de «alto/bajo»; en *Second Life*, simplemente no se puede violar la regla de los 15 metros. La regla forma parte del código y éste controla cómo somos en *Second Life*. No tenemos la opción de desobedecer la regla, al igual que no la tenemos de desobedecer la ley de la gravedad.

---

51 Lawrence Lessig, *Por una cultura libre. Cómo los grandes grupos de comunicación utilizan la tecnología y la ley para clausurar la cultura y controlar la creatividad*, Madrid, Traficantes de Sueños, 2005, pp. 21–23, discutiendo el proceso *United States vs. Causby*, U.S. 328, 1946, pp. 256, 261. El Tribunal concluyó que sólo podría alegarse «incautación» si el uso estatal de su tierra suponía una destrucción efectiva del valor del terreno de los Causby. Este ejemplo me lo sugirió el excelente artículo de Keith Aoki titulado «(Intellectual) Property and Sovereignty: Notes Toward a Cultural Geography of Authorship», *Stanford Law Review*, núm. 48, 1996, pp. 1293, 1333. Véase también Paul Goldstein, *Real Property*, Minneola (NY), Foundation Press, 1984, pp. 1112–1113.

52 St. George Tucker, *Blackstone's Commentaries 3*, South Hackensack (NJ), Rothman Reprints, 1969, p. 18.

Por lo tanto, el código es la ley aquí, y ese código/ley aplica su control directamente. Obviamente este código cambia (como la ley). La clave es reconocer que este cambio en el código se concibe (a diferencia de las leyes de la naturaleza) con el fin de reflejar las decisiones y los principios de los desarrolladores de dicho código.

Consideremos otra ilustración del mismo argumento. Como he dicho, *Second Life* concede a sus residentes los derechos de propiedad intelectual sobre los objetos que diseñan allí —propiedad que abarca tanto el interior como el exterior de *Second Life*.[53] (Tal como describía uno de sus fundadores: «Nuestros abogados se llevaron las manos a la cabeza, pero nosotros decidimos que el futuro de nuestra compañía no pasaba por apropiarnos de lo que crearan nuestros usuarios»).[54] Eso mismo sucede con la propiedad intelectual en el espacio real: a menos que optemos por ceder nuestros derechos de autor a una corporación (¡no lo hagas!), cuando creamos algo en el espacio real, automáticamente se nos concede por ley el copyright sobre nuestra obra. En ambos espacios, asimismo, tenemos derecho a ceder esos derechos. Yo presido una entidad no lucrativa llamada *Creative Commons*, la cual facilita que los creadores indiquen qué libertades quieren que vayan aparejadas a su creatividad. En el espacio real, cuando utilizamos una licencia *Creative Commons*, marcamos nuestro contenido con la licencia que preferimos, de modo que los usuarios sean conscientes de las libertades que tienen. Y si se violan los términos recogidos en dicha licencia, es la Ley de Copyright la que acude en nuestra defensa.

Second Life ha llevado esta idea un paso más allá. Los creadores de *Second Life* pueden marcar su contenido con la licencia que prefieran. Ahora bien, los administradores de este mundo están explorando la idea de que la licencia escogida pueda afectar de forma directa a lo que otros pueden hacer con esa creatividad. Si el contenido está marcado con una licencia *Creative Commons*, entonces alguien puede fotografiarlo sin necesidad de permiso expreso; pero si no está marcado con una licencia, entonces el objeto se volverá invisible si alguien intenta fotografiarlo. Aquí encontramos, una vez más, que el código impone su ley de un modo mucho más efectivo de lo que jamás podría hacerse en el espacio real.

---

53 J. D. Lasica, *Darknet: Hollywood's War Against the Digital Generation*, Nueva York, Wiley, 2005, p. 248 [ed. cast.: *Darknet: la guerra contra la generación digital y el futuro de los medios audiovisuales*, trad. por María Lourdes Silveira Lanot, Madrid, Editorial Nowtilus, 2006].

54 *Ibidem*, p. 246.

Internet

Por más que, como ya dije, podamos distinguir entre el ciberespacio e Internet, el argumento que vengo defendiendo con respecto al primero es igualmente válido para ésta última. Hay determinados atributos arquitectónicos de Internet que llevan inscritos ciertos principios. Esos atributos también pueden cambiar, y si lo hacen, los principios que promueve Internet serán diferentes.

El ejemplo más significativo de ello es uno que sólo mencioné en la primera edición de este libro, pero que fue uno de los ejes de mi siguiente obra, *The Future of Ideas*. Se trata del principio de comunicación «punto a punto» descrito por los arquitectos de redes Jerome Saltzer, David Clark y David Reed en 1981.[55] Este principio constituye una filosofía de diseño acerca de cómo deberían construirse las redes. Su consejo es mantener la mayor simplicidad en la arquitectura de redes, transfiriendo toda la inteligencia que se necesite a los extremos de la red, o puntos, al menos en la medida de lo posible.

Como ya he descrito, Internet plasmó este principio mediante una limitación muy estrecha de la funcionalidad del conjunto de protocolos TCP/IP —esto es, teniendo como única función la distribución optimizada de paquetes de datos. Lo que contengan esos paquetes o a quién vayan dirigidos no es de la incumbencia de dicho protocolo, cuyo único fin es distribuirlos.

Una de las consecuencias de este diseño es, pues, que la gente puede innovar en Internet sin necesidad alguna de coordinarse con el propietario de la red de turno. Si alguien desea desarrollar una aplicación de voz sobre IP, lo único que tiene que hacer es escribirla de modo que el envío de datos a través de la red funcione con el conjunto de protocolos TCP/IP.

Tal diseño lleva inscrito un principio que alienta la innovación de las aplicaciones de esta red; y esto tanto porque minimiza los costes del desarrollo de nuevas aplicaciones (librando al innovador del engorro de pedir permiso a todo el mundo) como porque impide conductas estratégicas por parte del propietario de la red. Consideremos de nuevo la idea de desarrollar

---

55 Véase Jerome H. Saltzer *et al*., «End-to-End Arguments in System Design», en Amit Bhargava(ed.), *Integrated Broadband Networks*, Nueva York, Elsevier Science Publishing Co., 1991, p. 30.

una aplicación de telefonía vía Internet (VOIP). Si la red estuviera en manos de las compañías telefónicas, éstas no se sentirían entusiasmadas ante una aplicación que invade su mercado. Por lo tanto, si hubiera que pedir permiso antes de poder implementar la aplicación VOIP, podríamos tener la certeza de que ésta no se implementaría —bien porque fuera bloqueada, bien porque, simplemente, los astutos desarrolladores pensaran que era una pérdida de tiempo desarrollar una aplicación que iba a terminar siendo bloqueada. Como describe Susan Crawford: «El milagroso crecimiento de Internet ha provenido en gran medida de la ausencia de discriminación contra los niveles superiores. [...] Los innovadores de la capa de aplicación han podido dar por sentada la existencia estable y continuada de las capas inferiores».[56]

En este caso, los principios privilegiados son la innovación y la competencia. La red potencia la gama más amplia de innovadores que pueda existir —sus propios usuarios—, autorizando a todos ellos a innovar para dicha red. Cualquier innovación puede implementarse en la red (con tal de que respete el conjunto de protocolos TCP/IP); y si a sus usuarios les convence, entonces esa innovación será un éxito.

Simultáneamente —al menos siempre que se respete el principio de comunicación punto a punto—, este diseño inhabilita al actor potencialmente más poderoso de una red, su propietario, para interferir en la oportunidad de innovación que contiene la red. Puede que a aquél no le agrade lo que se desarrolla, pero el principio de comunicación punto a punto le priva de la oportunidad de bloquear dicho desarrollo.

Ahora bien, del mismo modo que se podía transformar efectivamente la red TCP/IP original de modo que fuera posible cubrir sus «lagunas» informativas, también se la podría transformar para eliminar este principio. Es más, las herramientas descritas en el Capítulo 4 podrían provocar este efecto. Por ejemplo, el propietario de una red podría escanear los paquetes que atravesaran su red y bloquear aquéllos que no provinieran de una aplicación conocida o aprobada. Para figurar en la lista de aplicaciones permitidas, sus desarrolladores tendrían que contactar con el propietario y solicitarle su inclusión en dicha lista. Tal cambio en el modo de funcionar de Internet es completamente posible desde un punto de vista técnico, y, de hecho, ya se está trabajando en versiones, tanto por motivos de seguridad como de

---

56 Susan P. Crawford, «Symposium, Law and the Information Society, Panel V: Responsibility and Liability on the Internet, Shortness of Vision: Regulatory Ambition in the Digital Age», *Fordham Law Review*, núm. 74, 2005, pp. 695, 700–701.

competencia. Y es que algunas redes, ávidas por controlar los tipos de aplicaciones que funcionan en ellas por razones competitivas, podrían recurrir a dichos cambios para bloquear aplicaciones que les resultan desfavorables (una vez más, pensemos en las compañías telefónicas bloqueando las aplicaciones VOIP). Otras, ansiosas por evitar los virus y otros problemas en su red, podrían simplemente optar por no complicarse la vida y bloquear todas las aplicaciones. Uno u otro motivo produciría el mismo resultado: la innovación en Internet quedaría sofocada.

Al igual que las historias acerca del «ciberespacio», este caso centrado en Internet también demuestra el vínculo entre arquitectura y política. El principio de comunicación punto a punto es un paradigma tecnológico que lleva inscritos unos principios. La decisión acerca de qué arquitectura impulsar es una decisión acerca de qué políticas impulsar, y esto es cierto incluso en el contexto en el que Internet no es un «lugar»— incluso cuando «sólo» es un medio.

Cómo influyen las arquitecturas y difieren los espacios

Los espacios que he descrito hasta aquí son diferentes. En algunos lugares, se da una comunidad —un conjunto de normas que los miembros de la comunidad se atribuyen y cumplen. Rasgos como la visibilidad (como opuesta al anonimato) y la perdurabilidad contribuyen a crear esas normas; el anonimato, la transitoriedad y la diversidad hacen más complicado crear comunidad.

En lugares donde los miembros de una comunidad no respetan por sí mismos las normas, éstas son complementadas con leyes impuestas, bien mediante el código, bien por parte de una soberanía relevante. Estos complementos pueden favorecer alguna finalidad normativa, pero a veces pueden también entrar en tensión con el objetivo de construcción de comunidad.

Si tuviéramos que simplificar esta diversidad de espacios mediante la identificación de una dimensión que nos permitiera clasificarlos, ésta bien podría ser la de la susceptibilidad al control que presenta cada uno de los grupos. Algunos de ellos pueden controlarse simplemente mediante normas —*.law.cyber*, por ejemplo. La única tecnología apta para modificar la conducta allí —asumiendo mi compromiso de no vigilar ni punir la mala

conducta— eran las normas de mis estudiantes de la Facultad de Derecho. Otros grupos son susceptibles de verse afectados por otras tecnologías de control. Es más, a medida que pasamos de *.law.cyber* a CC, de ahí a *Lambda MOO*, de ahí a AOL y de ahí a *Second Life*, se va incrementando la capacidad de usar estas otras tecnologías de control, por más que dicha capacidad, por supuesto, se vea restringida por la competencia. Si el código le quita todo el atractivo a un lugar, la gente lo abandonará.

Así pues, en CC y AOL los arquitectos podían servirse de la tecnología para modificar la conducta. Ahora bien, si los cambios se alejan mucho de lo que la mayoría de los miembros consideran que es el sentido del espacio, éstos simplemente pueden abandonarlo. La amenaza de esta restricción fomenta la aparición de alternativas, por supuesto. A medida que los *blogs* florecen, a un espacio como CC le va quedando un poder de mercado relativamente pequeño. La cuestión se complica al referirnos al poder de mercado de AOL. Sin duda, existen muchos otros PSI pero, una vez que alguien se hace miembro de uno, los costes de pasarse a otro resultan significativos.

La historia se complica aún más en *LambdaMOO*. En realidad, nada liga a la gente a un MOO concreto (hay cientos de ellos, y la mayoría son gratuitos). Ahora bien, dado que los personajes de un MOO hay que ganárselos más que comprarlos, y dado que esto lleva su tiempo y que los personajes no son fungibles, a los miembros de un MOO de éxito les cuesta cada vez más marcharse a otro. Tienen todo el derecho a hacerlo, pero en el mismo sentido en que los ciudadanos soviéticos tenían derecho a marcharse del país —a saber, dejando atrás todos los bienes que habían ganado en su mundo particular.

Finalmente, *Second Life* es un espacio susceptible de un mayor control. El código regula la experiencia en *Second Life* más que en cualquiera de los otros cuatro espacios, y la intimidad de la experiencia en *Second Life* arrastra a la gente dentro del espacio y hace muy costosa la salida. Una vez más, existen límites al control, pero éste está articulado de forma más refinada que en cualquiera de los otros contextos. Y si hemos de creer a Philip Rosedale, el Director Ejecutivo de *Second Life*, el control mediante el código en este espacio se hará más sutil. Así me lo describía él:

> Nuestra opinión es [...] que deberíamos pasarnos firmemente al código, en la medida en que podamos, ya que nos proporciona una elevada capacidad de crecimiento. Y sólo cuando sea absolutamente necesario o inevitable,

deberíamos ejecutar políticas al margen del código. Hay cosas que observamos y sobre las que nos decimos: «Bueno, algún día podremos arreglar esto mediante el código, pero, por ahora, nos limitaremos a hacerlo a mano».[57]

Regulando el código para regular mejor

He examinado un conjunto de ciberespacios para aclarar los elementos de regulación que operan en cada uno de ellos; entre estos elementos de regulación, el código cobra cada vez mayor importancia. En el ciberespacio en particular y, en general en toda Internet, el código lleva inscritos principios y posibilita, o no, un cierto grado de control. Más aún, tal y como hemos visto en esta parte, el código constituye en sí mismo una herramienta de control —no de control estatal, al menos en los casos que he examinado, sino de control al servicio de los fines de cualquier soberanía que lo escriba.

Estas historias sugieren una técnica que, una vez comprendida, podremos reconocer en muchos contextos de regulación diferentes. Si *Second Life* puede usar el código para controlar mejor la conducta, ¿qué sucederá en la *primera vida*? Si America Online puede usar el código para controlar mejor el fraude, ¿qué sucederá en América *offline*? Si Internet puede usar el diseño de comunicación punto a punto para favorecer mejor la competencia, ¿qué enseña esto a los reguladores en la materia? ¿Cómo orientan estas técnicas la práctica de los diseñadores de políticas?

La respuesta es que éstos últimos vienen haciendo lo mismo en el espacio real desde hace mucho tiempo. Así como el Capítulo 5 describí cómo el código servía para hacer más regulable la conducta, ahora veremos cómo los reguladores ya han empleado el código para controlarla de forma directa. Consideremos unos cuantos ejemplos obvios:

57 Grabación de audio: entrevista con Philip Rosedale (16 de enero de 2006; incluido en el archivo del autor).

Cintas de audio

La característica más significativa de los medios digitales es que posibilitan la obtención de copias perfectas, ya que están conformados simplemente por datos, y éstos no son más que una serie de unos y ceros. Los ordenadores tienen complejos algoritmos para verificar que cuando han copiado una serie de datos, han copiado exactamente esa serie de datos.

Tal característica genera, así, un nuevo riesgo para los «vendedores de contenido». Mientras que el código de la tecnología de copia analógica implicaba que la copia siempre sería una versión degradada del original, el código de las tecnologías digitales implica que la copia puede ser idéntica al original. Por consiguiente, la amenaza que suponen las «copias» para los proveedores de contenidos es mayor en el mundo digital que en el analógico.

La tecnología de la DAT (*Digital Audio Tape*, Cinta de Audio Digital) fue la primera en mostrar este riesgo. Al igual que cualquier grabación digital, la DAT puede, en principio, copiar contenidos de forma perfecta. Los proveedores de contenidos se aterrorizaron pensando que la piratería de las DAT destruiría su industria, por lo que presionaron de forma efectiva al Congreso para promulgar leyes adicionales que les protegieran de la amenaza digital.

El Congreso podría haber respondido a sus demandas de muchas maneras. Podría haber empleado la ley para regular directamente la conducta, aumentando las penas por la copia ilegal; podría haber subvencionado una campaña publicitaria oficial contra la copia ilegal, o bien programas escolares para disuadir a los estudiantes de comprar ediciones pirateadas de discos famosos; podría haber impuesto un canon sobre las cintas vírgenes y transferirlo luego a los propietarios de material bajo copyright;[58] o podría haber intentado regular la tecnología DAT para debilitar la amenaza que planteaba al copyright.

58 Véase Lessig, *Por una cultura libre*, *op. cit.*, p. 296, nota 13: «La propuesta de Fisher es muy similar a la propuesta de Richard Stallman para DAT. A diferencia de la de Fisher, la propuesta de Stallman no pagaría a los artistas de un modo directamente proporcional, si bien los artistas más populares ganarían más que los menos populares». Véase http://www.wired.com/wired/archive/1.03/1.3_stallman.copyright.html.

El Congreso optó por estas dos últimas respuestas. La *Audio Home Recording Act* (Ley de Grabaciones de Audio Domésticas) impuso un canon a las cintas vírgenes y reguló directamente el código de las tecnologías de reproducción digital. Esta ley exige a los productores de dispositivos de grabación digital la instalación en sus sistemas de un chip que implementa un sistema codificado para vigilar las copias realizadas en esa máquina.[59] Este chip permite un número limitado de copias personales, si bien en las copias de otras copias la calidad de la grabación se vería degradada. En esencia, el Congreso exigió la modificación del código de copia digital para restaurar las imperfecciones «naturales» del código anterior.

Una vez más, nos encontramos con que el Congreso regula el código como un medio de regular la conducta —ordenando que las copias múltiples sean imperfectas como un medio de minimizar el número de copias ilegales. Del mismo modo que sucedía con la telefonía, esta regulación tiene éxito porque el número de fabricantes de tecnología DAT es relativamente reducido. Una vez más, dado un grupo objetivo de regulación limitado, la regulación estatal puede ser efectiva y propiciar una mayor regulabilidad de la conducta originalmente perseguida —la infracción del copyright.

Televisiones

A mediados de la década de los noventa, la preocupación de los padres por el efecto que la violencia televisiva ejercía sobre sus hijos había despertado la atención del Congreso, que respondió mediante la legislación. Ahora bien, las condiciones impuestas por la Primera Enmienda le habrían puesto muy difícil al Congreso bloquear la violencia televisiva de forma directa, por lo que buscó un modo de hacerlo indirectamente. De este modo, se exigió a los canales de televisión que etiquetasen su contenido indicando el nivel de violencia que contenía, y se ordenó a la industria televisiva desarrollar una tecnología que bloqueara el contenido en función de dichas etiquetas.

---

59 Véase *Audio Home Recording Act*, 17 USC 1002 1994 (exigiendo el sistema de gestión de copia en serie); véase también U.S. Department of Commerce, *Intellectual Property and the National Information Infrastructure: Report of the Working Group on Intellectual Property Rights*, Washington, DC: Information Infrastructure Task Force, 1995, pp. 179, 189–90.

Tal tecnología fue el «Chip V», impuesto como parte de la *Telecommunications Act* de 1996 (Ley de Telecomunicaciones).[60] Este chip facilitaría el bloqueo automático de las emisiones de televisión, basándose en criterios de contenido no del todo precisados todavía. Las propuestas más toscas implican algo parecido al sistema de calificación de la MPAA (*Motion Picture Association of America*, Asociación Cinematográfica de Estados Unidos); las más sofisticadas imaginaban selecciones basadas en un conjunto de factores mucho más variados.

Una vez más, el Congreso regula el código para influir en una conducta determinada (la emisión de programas televisivos violentos) en lugar de regular directamente dicha conducta. La dificultad de regular directamente constituye aquí igualmente un problema, si bien en este contexto proviene de límites constitucionales, no de la incapacidad para seguir la pista a quienes son regulados por la tecnología. La restricción consagrada en la Constitución empujó al Congreso a exigir tecnologías que otorgaran poder a los padres para discriminar contenidos televisivos. De este modo, el Congreso contenía un mal (la exposición a la violencia) que no puede regular directamente en virtud de la Constitución.[61]

Anti elusión [Anti circumvention]

Sean cuales sean los problemas de la industria de contenido con las cintas DAT, no cabe duda de que no son nada en comparación con los que tienen con los contenidos digitales e Internet. Aunque las cintas DAT posibilitan la obtención de copias perfectas, no facilitan en nada su distribución, recayendo ese honor en la Red. En este momento, la tecnología digital no sólo garantiza copias perfectas del contenido original, sino que también simplifica la distribución gratuita de dichas copias digitales.

---

60 Véase 47 CFR 15.120; véase también *Telecommunications Act* de 1996 Pub.L. 104–104, 551, 110 Stat. 56, 139–42, 1996, 47 USC 303, 1998 (acerca del estudio e implementación de dispositivos de bloqueo de video y de sistemas de calificación).

61 La consecuencia de implantar un Chip V eficaz en la mayoría de los televisores sería la eliminación de la típica justificación para regular el contenido de las emisiones televisivas. Si los usuarios se filtran a sí mismos, entonces la Comisión Federal de Comunicaciones no tiene que hacerlo por ellos; véase Peter Huber, *Law and Disorder in Cyberspace: Abolish the FCC and Let Common Law Rule the Telecosm*, Nueva York, Oxford University Press, 1997, pp. 172–173.

Como describiré en profundidad en el Capítulo 10, las tecnologías de «gestión digital de derechos» (DRM, por las siglas en inglés de *Digital Rights Management*) constituyen una respuesta a esta «característica» de las tecnologías digitales. Dichas tecnologías agregan un código al contenido digital que inhabilita la capacidad de copiarlo o distribuirlo —a no ser que la propia tecnología DRM lo permita técnicamente.

En consecuencia, las canciones que he comprado y descargado de la tienda musical de iTunes están protegidas por la tecnología DRM «de juego limpio» de Apple. Esta tecnología me permite copiar una canción a un número limitado de máquinas, restringiendo mi capacidad de hacerlo a una escala mayor, todo ello a través del código. La capacidad de «copia» es producto del código, y la tecnología DRM viene a modificar, o a matizar, tal capacidad. Se trata, pues, de un ejemplo clásico de implementación de un código que restituye el control sobre algo que el propio código (una variante) había impedido controlar hasta ese momento.

Estos sistemas DRM fueron creados por entidades privadas, pero en 1998 recibieron un importante respaldo por parte del Congreso. En la DMCA (*Digital Millennium Copyright Act*, Ley de Copyright del Milenio Digital), el Congreso prohibió la creación y distribución de tecnologías «producidas con el propósito de eludir una medida tecnológica que controle de modo efectivo el acceso» a una obra sujeta a copyright, o «diseñadas o producidas primordialmente con el propósito de evitar la protección ofrecida por una medida tecnológica que salvaguarde de modo efectivo el derecho del propietario del copyright».[62] Al prohibir este tipo de código, el Congreso pretendía incrementar el apoyo al código que los creadores de contenido estaban distribuyendo para proteger sus obras. De esta manera, a través de la regulación directa del código, el Congreso regulaba indirectamente las infracciones del copyright.

Desde que se promulgó esta ley, se han desencadenado un sinfín de conflictos y litigios alrededor de estas tecnologías: el primero data de 1999, cuando la Asociación de Control de Copias de DVD comenzó a demandar a particulares y sitios web que facilitaban el acceso al programa DeCSS, que podría emplearse para descifrar los datos de un DVD;[63] en julio de 2001,

62 *Digital Millenium Copyright Act*, 17 U.S.C., Secciones 512, 1201–1205, 1201(a)(2), 1201(b)(1)(A), 1998.

63 Véase *Electronic Frontier Foundation*, «DVD-CCA vs. Bunner and DVD-CCA vs. Pavlovich», disponible en http://www.eff.org/IP/Video/DVDCCA_case/. *DVD Copy Control Association, Inc. vs. Bunner,* 31 Cal. 4Th 864, Cal. 2003; *Pavlovich vs. Superior Court,* 29 Cal. 4Th 262, Cal. 2002; *Universal Studios, Inc. vs. Corley,* 273 F.3d 429, 2d Cir. 2001.

un programador ruso de 27 años llamado Dmitry Sklyarov fue arrestado mientras pronunciaba una conferencia en Las Vegas porque la compañía para la que trabajaba en Rusia había producido un software que permitía sortear las tecnologías de protección de acceso insertas en el sistema de libros electrónicos de Adobe.[64] Sklyarov pasó seis meses en una cárcel estadounidense antes de que se le permitiera reunirse con su familia en Rusia.

El efecto de esta regulación es difícil de medir. La *Electronic Frontier Foundation* ha detallado su visión del efecto de la ley cinco años después de su promulgación,[65] y por más que esta visión pueda no ser universal, sí que resulta universal la sorpresa ante el repertorio de casos que han sido llevados a juicio amparándose en dicha ley. (Dudo mucho que los redactores de la DMCA imaginaran que los fabricantes de puertas de garaje se ampararían en ella para proteger de la competencia sus sistemas de apertura automática. Finalmente perdieron).[66]

Banderas de emisión

A medida que aumenta la penetración de la televisión digital, los titulares de derechos de autor se muestran más preocupados por el riesgo que supone la emisión digital de contenido bajo copyright. Y es que, a diferencia de lo que sucedía con la televisión analógica, la calidad de la emisión digital es perfecta, de modo que las copias realizadas a partir de ella podrían ser igualmente perfectas. Y la distribución de copias perfectas de emisiones digitales en una red digital libre (Internet) es algo que aterra a los titulares de derechos de autor.

Su respuesta ha sido similar a la que dieron a las tecnologías DAT. Primero en la Comisión Federal de Comunicaciones y ahora en el Congreso, los titulares de derechos de autor han presionado al Gobierno para que decrete que cualquier tecnología capaz de reproducir emisiones digitales

---

64 Hay un archivo sobre Dmitri Sklyarov, su arresto y su juicio, disponible en http://www.freesklyarov.org/.

65 *Electronic Frontier Foundation*, «Unintended Consequences: Seven Years Under the DMCA», disponible en http://www.eff.org/IP/DMCA/?f=unintended_consequences.html.

66 Véase *Chamberlain Group, Inc. vs. Skylink Technologies*, Inc., 544 U.S. 923, 2005.

sea diseñada de modo que respete una «bandera de emisión» [*broadcast flag*]. Así, si la bandera está activada, la tecnología debe bloquear cualquier copia de ese contenido. Por lo tanto, se podría reproducir el contenido, pero no copiarlo. Tal y como lo describe Susan Crawford:

> La ley de banderas de emisión, destilada hasta su esencia, es un decreto por el que todos los fabricantes de productos electrónicos de consumo y todas las compañías dedicadas a la tecnología de la información han de garantizar que cualquier dispositivo que tenga contacto con el contenido de la televisión digital «reconozca y permita aplicar» la bandera, protegiendo el contenido contra su redistribución no autorizada. La Comisión Federal de Comunicaciones sostuvo que esta ley protegería las emisiones de la televisión digital («DTV») de la redistribución masiva a través de Internet.[67]

Hay mucho que decir acerca de la bandera de emisión, y casi nada sería bueno si fuera yo quien lo dijera.[68] Sin embargo, para el propósito de nuestro análisis, es la forma de la bandera de emisión la que es relevante, y no su sustancia. Estamos, así, ante el ejemplo más directo de regulación del código diseñada para controlar una conducta: la ley regula el código para mejorar la conducta.

En todos los casos que hemos examinado, el Estado actúa sobre un intermediario que tiene cierto poder sobre el código con el fin de modificar dicho código para producir un cambio de conducta. Que esta maniobra surta efecto dependerá del poder que tenga la aplicación concreta. Así, si se trata de un MOO, o de un espacio de discusión en red como *Counsel Connect*, la capacidad de controlar la conducta se verá significativamente limitada; si la aplicación es AOL o *Second Life*, los costes de abandonar el espacio podrían resultar bastante elevados para su usuario, con lo que el alcance de la regulación efectiva sería mayor; y si la aplicación es Internet, o cualquier tecnología digital producida o vendida en EEUU, entonces el poder del regulador sería aún más amplio. El código se convierte en ley incluso si persiste la capacidad de escapar a la regulación de dicho código.

---

67 Crawford, «Symposium, Law and the Information Society, Panel V», *op. cit.*, núm. 695, p. 710.

68 El coste más significativo de esta tecnología recae en la innovación. Si la exigencia de esta bandera de emisión se extiende hasta abarcar cualquier dispositivo capaz de descodificar la señal de televisión digital, entonces tal exigencia afectaría a cualquier dispositivo digital en red. Sería la primera vez que las aplicaciones de red tendrían que cumplir con un mandato técnico de tal amplitud que supondría un obstáculo infranqueable para el desarrollo del software de código abierto y del software libre.

Estos ejemplos apuntan a una cuestión general acerca del funcionamiento de la regulación que requiere muchas matizaciones significativas. Para captar el efecto que los requisitos del código tienen sobre cualquier política de regulación será necesaria, como escribe Polk Wagner, una comprensión que sea «profundamente dinámica».[69] Parte de esa dinámica pasa, por supuesto, por la resistencia. Los individuos pueden actuar para resistirse a la fuerza del código de modo directo o a través del propio código. Tal y como Tim Wu ha descrito acertadamente, el código por sí mismo no necesariamente incrementa la regulación —el código puede usarse también para sortearla. Una pistola es un trozo de código que hace maravillas en lo que a destruir la paz se refiere; las tecnologías de elusión [*circumvention technologies*] también son código, y permiten debilitar las leyes que refuerzan el control; y no otra cosa que código son los protocolos de compartición de archivos en redes de pares (P2P), los cuales socavan la efectividad de las regulaciones de derechos de autor que restringen la libertad de distribuir obras sujetas a copyright. Por lo tanto, para calibrar la efectividad de una regulación específica tendremos que considerar estas interacciones, así como la resistencia a través del código que se pueda generar. Wu lo explica así:

> El motivo por el que el código llega a tener importancia para la ley es su capacidad para definir la conducta a una escala masiva. Tal capacidad puede implicar restricciones en la conducta, en cuyo caso el código regula, pero también puede implicar el ajuste de dicha conducta a formas legalmente convenientes.[70]

En este segundo sentido, el código funciona «como un mecanismo antirregulador: una herramienta para minimizar los costes de la ley que ciertos grupos utilizarán en su provecho».[71]

De modo fundamental, estas complicaciones sugieren que es necesario disponer de un marco comprensivo de mayor amplitud. A lo largo de este capítulo, he destacado la interacción entre tecnología, política y ley, la cual sugiere un modelo mucho más vasto, que describo en el Capítulo 7. A continuación, en el Capítulo 8, retomaremos la dinámica de regulación mediante el código para considerar otra importante matización.

---

69 R. Polk Wagner, «On Software Regulation», *Southern California Law Review*, núm. 78, 2005,: pp. 457, 470–71. Véase también Joel R. Reidenberg, «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, núm. 153, 2005, p. 1951; Joshua A. T. Fairfield, «Cracks in the Foundation: The New Internet Legislation's Hidden Threat to Privacy and Commerce», *Arizona State Law Journal*, núm. 36, 2004, p. 1193 (defendiendo que el Congreso debería aplicar más la excepcionalidad jurisdiccional y menos la excepcionalidad de contenido en su regulación del ciberespacio).

70 Timothy Wu, «When Code Isn't Law», *Virginia Law Review*, núm. 89, 2003, pp. 679, 707–708.

71 *Ibidem*, p. 682.

7. Qué cosas regulan

John Stuart Mill, inglés de nacimiento, se convirtió en uno de los filósofos políticos más influyentes en EEUU. Sus escritos abarcan desde importantes trabajos de lógica hasta un texto sobre la igualdad de sexos, *El Sometimiento de las Mujeres*, que todavía hoy resulta estimulante; pero quizás la obra con mayor influencia hasta nuestros días sea un libro relativamente corto titulado *Sobre la libertad*. Publicado en 1859, esta poderosa defensa de la libertad individual y de la diversidad de ideas representa una importante panorámica del pensamiento progresista y liberal de la segunda mitad del siglo XIX.

Ahora bien, para nosotros, los estadounidenses, el término «liberal» [*libertarian*] tiene un significado específico que se suele asociar con ideas contrarias al Estado.[1] Desde la perspectiva del liberalismo moderno, éste constituye *la* amenaza para la libertad, y no la acción privada. Por lo tanto, el buen liberal centra su atención en reducir el poder estatal, asegurando que si se frenan los excesos del Estado, la libertad de la sociedad estará garantizada.

---

1 O, para ser más precisos, contra una cierta forma de regulación estatal. Los argumentos liberales más contundentes contra la regulación en el ciberespacio los ha propuesto, entre otros, Peter Huber en *Law and Disorder in Cyberspace*, *op. cit.*, donde el autor impugna la regulación por parte de la Comisión Federal de Comunicaciones y aboga por la regulación mediante el derecho consuetudinario *[common law]*. Véase también Thomas Hazlett, «The Rationality of U.S. Regulation of the Broadcast Spectrum», *Journal of Law and Economics*, núm. 33, 1990, pp. 133, 133–39. Para un abogado resulta difícil comprender a qué se refiere eso del «derecho consuetudinario», cuyas leyes son múltiples y cuyo contenido sustantivo ha cambiado. A los abogados nos gusta mitificar el proceso del derecho consuetudinario, en el que los jueces adoptan decisiones políticas en espacios pequeños y con el trasfondo de precedentes vinculantes. Puede que sea esto lo que Huber tiene en mente y, en ese caso, sin duda existen beneficios para el sistema; ahora bien, él mismo es consciente de que el derecho consuetudinario no es más que otra forma de regulación, por mucho que esté constituida de forma diferente.

La visión de Mill no fue tan estrecha; era un defensor de la libertad y un opositor a las fuerzas que la reprimían, pero estimaba que éstas no se reducían al Estado. Para él, la libertad se veía amenazada tanto por las normas como por el Estado, tanto por la estigmatización y la intolerancia como por la coacción de la punición estatal. El objetivo de Mill era alertar sobre las fuerzas coercitivas de índole privada; su obra constituyó una defensa contra las normas que constreñían la libertad, porque en la Inglaterra de su época las pautas sociales eran la auténtica amenaza para ésta.

Su método reviste una gran importancia y haríamos bien en adoptarlo nosotros también, formulándonos la siguiente pregunta: ¿cuál es la amenaza a la libertad y cómo podemos resistirnos a ella? Nótese que Mill no se limita a preguntar: ¿cuál es la amenaza *del Estado* a la libertad? Esta formulación entraña la comprensión de que no sólo el Estado es capaz de amenazar la libertad, y de que a veces esta amenaza puede proceder de la acción privada más que de la estatal. Lo que de verdad le importaba a Mill no era la fuente de la amenaza a la libertad, sino la propia libertad.

Las amenazas a la libertad varían con el tiempo. Puede que en la Inglaterra de finales del siglo XIX la principal amenaza a la libertad de expresión fueran las normas, pero dudo mucho de que sigan siéndolo hoy por hoy. En EEUU, durante las dos primeras décadas del siglo XX, la principal amenaza a la libertad de expresión fue la represión penal del Estado sobre los discursos impopulares; las fuertes protecciones garantizadas por la Primera Enmienda determinan que esa amenaza específica sea ahora menos significativa.[2] El movimiento obrero se fundó sobre la idea de que el mercado representa a veces una amenaza a la libertad —no tanto por los bajos salarios, sino porque la propia forma de organización del mercado impide ciertas clases de libertad.[3] En otras sociedades, en otras épocas, el mercado ha sido clave para la libertad, en lugar de ser su enemigo.

---

2 Los primeros ejemplos son las condenas dictadas en aplicación de la *Espionage Act* de 1917; véase, por ejemplo, *Schenck vs. United States*, 249 US 47, 1919 (ratificando la condena por la distribución de octavillas donde se arremetía contra el reclutamiento para la Primera Guerra Mundial); *Frohwerk vs. United States*, 249 US 204, 1919 (ratificando la condena a un periódico acusado de incitar a la deslealtad); *Debs vs. United States*, 249 US 211, 1919 (ratificando la condena contra un discurso político acusado de provocar insubordinación y deslealtad).

3 Véase, por ejemplo, la obra de John R. Commons, *Legal Foundations of Capitalism*, 1924, pp. 296–98, discutida en Herbert Hovenkamp, *Enterprise and American Law, 1836–1937*, Cambridge (Mass.), Harvard University Press, 1991, p. 235; véase también John R. Commons, *Institutional Economics: Its Place in Political Economy*, New Brunswick (NJ), 1934, reeditada por Transaction Publishers en 1990.

Por consiguiente, en lugar de pensar en abstracto en «el enemigo de la libertad», deberíamos concentrarnos en la amenaza concreta a la libertad que puede existir en una época dada y en un lugar concreto. Y todo esto es especialmente cierto cuando reflexionamos sobre la libertad en el ciberespacio. Estoy convencido de que el ciberespacio produce una nueva amenaza a la libertad, no nueva porque ningún teórico la haya contemplado antes,[4] sino por su reciente apremio. Vamos camino de comprender la emergencia de un nuevo y potente regulador en el ciberespacio. Este regulador podría suponer una amenaza significativa a una amplia variedad de libertades, y todavía no hemos entendido cómo llegar a controlarlo.

Este regulador es lo que yo llamo el «código» –las instrucciones inscritas en el software o en el hardware que hacen del ciberespacio lo que es. Este código es el «entorno construido» de la vida social en el ciberespacio, su «arquitectura».[5] Y si a mediados del siglo XIX la principal amenaza a la libertad fueron las normas, a comienzos del siglo XX el poder estatal y durante buena parte del siglo XX el mercado, mi tesis es que hemos de llegar a comprender cómo en el siglo XXI nuestra preocupación debería centrarse en un regulador diferente —el código.

---

4 La idea de que las correcciones espaciales minúsculas incorporan la aplicación de una disciplina, y que esta disciplina representa una regulación importante supone una mínima parte de la obra de Michel Foucault; véase *Discipline and Punish: The Birth of the Prison*, Nueva York, Vintage, 1979, pp. 170–177, aunque su obra inspira esta perspectiva de forma general [ed. cast.: *Vigilar y castigar: nacimiento de la prisión*, trad. por Aurelio Garzón del Camino, Madrid, Siglo XXI, 1994]. De estas ideas se ocupa Oscar Gandy en *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, Westview Press, 1993, p. 23. Por su parte, David Brin sostiene la tesis más amplia que yo defiendo aquí —que la amenaza a la libertad no se reduce a la amenaza por parte del Estado; véase *The Transparent Society*, *op. cit.*, p. 110.

5 Véase, por ejemplo, Tom J. Bartuska y Gerald L. Young (eds.), *The Built Environment: A Creative Inquiry into Design and Planning*, Menlo Park (Cal.), Crisp Publications, 1994; J. Mark Schuster *et al*. (eds.), *Preserving the Built Heritage: Tools for Implementation*, Hanover (NH), University Press of New England, 1997. En la teoría de diseño, la noción que estoy describiendo concuerda con la tradición de Andres Duany y Elizabeth Plater-Zyberk; véase, por ejemplo, William Lennertz, «Town-Making Fundamentals», en Andres Duany y Elizabeth Plater-Zyberk (eds.), *Towns and Town-Making Principles*, Nueva York, Rizzoli, 1991: «La obra de [...] Duany y [...] Plater-Zyberk parte del reconocimiento de que el diseño influye en la conducta. [Los autores] contemplan la estructura y el funcionamiento de una comunidad como interdependientes. Por este motivo, están convencidos de que las decisiones de un diseñador impregnarán las vidas de los residentes no sólo visualmente, sino en sus formas de vivir. Del mismo modo, creen que el diseño estructura las relaciones funcionales, tanto cuantitativa como cualitativamente, y constituye una herramienta sofisticada cuyo poder excede sus atributos cosméticos» (p. 21).

Esto no implica dejar de lado otros reguladores «significativos». No estoy defendiendo que sólo exista una amenaza a la libertad, o que debiéramos olvidar otras amenazas más tradicionales. Por el contrario, sostengo que hemos de añadir a la lista una amenaza cada vez más acuciante. Y estoy convencido de que para captar esta reciente amenaza, necesitamos una interpretación más amplia de cómo funciona la regulación —una que no se centre en la influencia que ejercen por separado el Estado, las normas o el mercado, sino que integre todos estos factores en un único esquema conjunto.

Este capítulo constituye un paso hacia esta interpretación más compleja,[6] una invitación a pensar más allá de la amenaza a la libertad por parte del Estado, un mapa para una comprensión más amplia.

La vida de un punto

Hay muchas maneras de pensar acerca de la «regulación», y me gustaría hacerlo desde la perspectiva de alguien que es regulado o, lo que es distinto, alguien que está sometido a restricciones. Ese alguien regulado es representado aquí mediante este (pobre) punto —una criatura (el lector o yo mismo) sometida a diferentes regulaciones que pueden restringir (o facilitar, como veremos) la conducta del punto. Mediante la descripción de las diversas restricciones que pueden afectar a este individuo, espero mostrar algo acerca del modo en que dichas restricciones funcionan conjuntamente.

He aquí, pues, el punto.

6 En otro lugar, he denominado esto la «Nueva Escuela de Chicago»; véase Lawrence Lessig, «The New Chicago School», *Journal of Legal Studies*, núm. 27, 1998, p. 661. Se enmarca dentro del «enfoque de las herramientas» de la acción estatal, aunque describe cuatro frente a las cinco herramientas que contemplan John de Monchaux y J. Mark Schuster, «Five Things to Do», en Schuster (ed.), *Preserving the Built Heritage*, *op. cit.*, p. 3. En el «Apéndice» de la presente obra, desarrollo esta hipótesis general de las cuatro herramientas de regulación.



¿Cómo es «regulado» este punto?

Comencemos con algo fácil: fumar. Si deseamos fumar tabaco, ¿con qué restricciones nos encontramos? ¿Qué factores regulan nuestra decisión de fumar o no?

Una restricción es de índole legal. Al menos en algunos lugares, la ley regula el acto de fumar —en EEUU, la ley prohíbe vender cigarrillos a los menores de dieciocho años, y sólo permite venderlos a adultos menores de veintiséis si acreditan su edad con un documento de identidad. La ley también regula dónde se permite fumar —no se puede fumar en el aeropuerto O'Hare de Chicago ni tampoco en el interior de un avión o de un ascensor, por ejemplo. Así pues, la ley procura controlar la conducta de fumar, al menos de estas dos maneras, operando como un tipo de restricción sobre el individuo que desea fumar.

Pero la ley no es la restricción más significativa a la que se enfrentan los fumadores estadounidenses, quienes ciertamente sienten regulada su libertad, aunque sólo rara vez por parte de la ley. No existe una policía de fumadores y los tribunales que se ocupan de esta cuestión son todavía muy raros. Los fumadores estadounidenses están más bien limitados mediante normas: normas que dicen que uno no enciende un cigarrillo en el interior de un coche privado sin antes pedir permiso al resto de pasajeros, y también que no hace falta pedir permiso para fumar en un picnic; normas que dicen que otras personas te pueden pedir que dejes de fumar en un restaurante, y también que nunca se debe fumar durante una comida. Estas normas ejercen una cierta restricción y regulan la conducta de los fumadores.

Con todo, las leyes y las normas no son las únicas fuerzas que operan sobre el acto de fumar. El mercado también impone su restricción, puesto que el precio de los cigarrillos limita nuestra capacidad de fumar —si este precio cambia, también lo hace la restricción. Lo mismo sucede con respecto a

la calidad. Si el mercado provee una variedad de cigarrillos de una amplia gama de calidades y precios, nuestra capacidad para seleccionar el tipo de cigarrillos que nos gusta se incrementa; en este caso, si aumentan las opciones, se reduce la restricción.

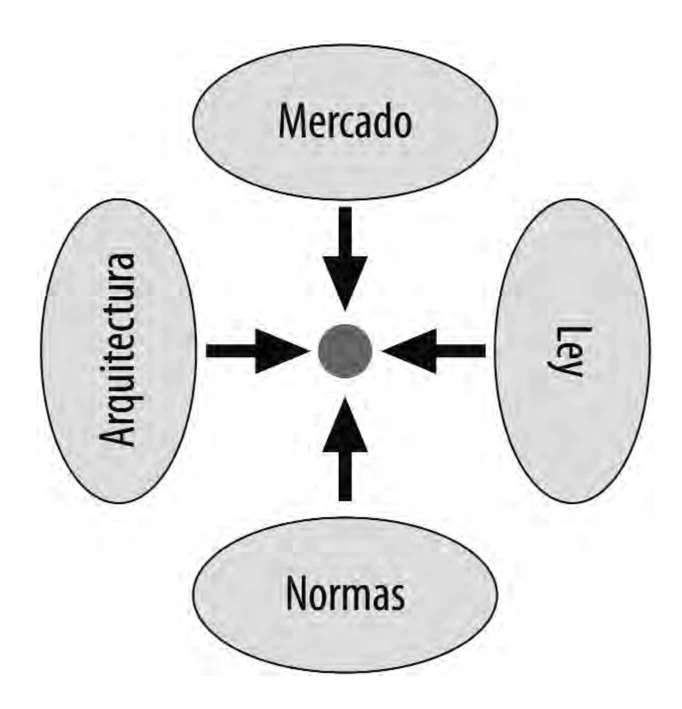
Finalmente, existen restricciones creadas por la tecnología de los cigarrillos, o por las tecnologías que afectan a su suministro.[7] Los cigarrillos con nicotina resultan adictivos y, en consecuencia, suponen una restricción mayor que los que no llevan nicotina. Los cigarrillos que no producen humo representan una restricción menor, ya que se pueden fumar en más lugares, al contrario que los cigarrillos que desprenden un fuerte olor, que suponen una mayor restricción al poderse fumar en menos sitios. Cómo es el cigarrillo, cómo está diseñado, cómo está construido —en una palabra, su arquitectura—, todo ello influye en las restricciones a las que se enfrenta un fumador.

Por consiguiente, cuatro son las restricciones que regulan a este pobre punto —la ley, las normas sociales, el mercado y la arquitectura—, y la «regulación» ejercida sobre él será la suma de todas ellas. Los cambios en cualquiera de ellas influirán en el conjunto de la regulación. Algunas restricciones se respaldarán entre sí, mientras que otras pueden llegar a anularse. Por lo tanto, «los cambios tecnológicos pueden preceder a los cambios en [...] las normas»,[8] y viceversa. Una visión completa, pues, habrá de considerar estas cuatro modalidades conjuntamente.

Pensemos este conjunto de restricciones del siguiente modo:

7 A su vez, estas tecnologías se ven afectadas, sin duda, por el mercado. Obviamente, estas restricciones no podrían existir independientemente unas de otras, sino que se afectan entre sí otras de modos significativos.

8 Lasica, *Darknet*, *op. cit.*, p. 16. Véase también Lior Jacob Strahilevitz, «Charismatic Code, Social Norms and the Emergence of Cooperation on the File-Swapping Networks», *Virginia Law Review*, núm. 89, 2003, p. 505 (argumentando que el código «carismático» crea una ilusión de reciprocidad que da cuenta de por qué la gente contribuye a una red de intercambio de archivos).



En este dibujo, cada uno de los óvalos representa una clase de restricción que opera sobre nuestro pobre punto, situado en el centro. Cada restricción le impone un coste diferente por llevar a cabo la conducta en cuestión —en este caso, fumar. El coste derivado de las normas es diferente del derivado del mercado, el cual a su vez difiere del derivado de la ley y del derivado de la (cancerígena) arquitectura de los cigarrillos.

Ahora bien, por más que difieran las restricciones, todas son claramente interdependientes. Cada una puede respaldar u oponerse a otra. Las tecnologías pueden socavar las normas y las leyes, pero también pueden respaldarlas. Algunas restricciones posibilitan que aparezcan otras, mientras que otras lo hacen imposible. Las restricciones operan conjuntamente, aunque cada una funcione de forma diferente y provoque un efecto distinto. Las normas restringen por la estigmatización que impone una comunidad; el mercado, por medio del precio que exige; las arquitecturas, a través de las constricciones físicas que imponen; y la ley, mediante el castigo con que amenaza.

Podemos calificar cada una de estas restricciones de «regulador» y concebirlas así como distintas modalidades de regulación. Cada modalidad posee una naturaleza compleja y resulta laborioso describir la interacción que se da entre ellas. En el apéndice de esta obra, he abordado esta complejidad de forma más completa. Por ahora, no obstante, basta con que veamos que las cuatro modalidades están vinculadas entre sí y que, en cierto sentido, se combinan para producir la regulación a la que se ve sometido, en cualquier ámbito, nuestro pobre punto.

Podemos usar el mismo modelo para describir la regulación de la conducta en el ciberespacio.[9]

La ley regula la conducta en el ciberespacio. Las leyes referidas al copyright, a la difamación y a la obscenidad suponen sanciones a posteriori para los que violan estos derechos legales. Cómo de bien o con qué eficacia regula la ley son otras cuestiones; en algunos casos lo hará de forma más eficaz, en otros, menos. Sea como sea, la ley continúa amenazando con una determinada consecuencia si se la desafía. Las asambleas legislativas promulgan leyes,[10] los fiscales acusan[11] y los tribunales condenan.[12]

También las normas regulan en el ciberespacio. Pruebe el lector a hablar de las políticas del Partido Demócrata en el grupo de noticias de costura alt.knitting y se verá expuesto a los mensajes iracundos de sus suscriptores; realice una «parodia» de la identidad de algún miembro de un MUD y puede que acabe «repudiado»;[13] hable sin parar en una lista de discusión y lo más probable es que sus mensajes acaben eliminados mediante un «filtro de majaderos» [*bozo filter*]. En cada uno de estos casos, un conjunto de sobrentendidos restringe la conducta, de nuevo mediante la amenaza de sanciones a posteriori impuestas por una comunidad.[14]

---

9 Jay Kesan ha ofrecido un análisis semejante, pero más exhaustivo. Véase Jay P. Kesan y Rajiv C. Shah, «Shaping Code», *Harvard Journal of Law and Technology*, núm. 18, 2005, pp. 319, 338.

10 Véase Michelle Armond, «Regulating Conduct on the Internet: State Internet Regulation and the Dormant Commerce Clause», *Berkeley Technology Law Journal*, núm. 17, 2002, pp. 379, 380.

11 Véanse, por ejemplo, las políticas del Fiscal General de Minnesota acerca de la jurisdicción de este Estado sobre aquéllos que transmitan información sobre apuestas a sus ciudadanos: http://web.archive.org/web/20000816215338/http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html.

12 Véase, por ejemplo, *Playboy Enterprises vs. Chuckleberry Publishing, Inc.,* 939 FSupp 1032, SDNY 1996; *United States vs. Thomas,* 74 F3d 701, 6º Cir. 1996; *United States vs. Miller,* 166 F3d 1153, 11º Cir. 1999; *United States vs. Lorge,* 166 F3d 516, 2º Cir. 1999; *United States vs. Whiting,* 165 F3d 631, 8º Cir. 1999; *United States vs. Hibbler,* 159 F3d 233, 6º Cir. 1998; *United States vs. Fellows,* 157 F3d 1197, 9º Cir. 1998; *United States vs. Simpson,* 152 F3d 1241, 10º Cir. 1998; *United States vs. Hall,* 142 F3d 988, 7º Cir. 1998; *United States vs. Hockings,* 129 F3d 1069, 9º Cir. 1997; *United States vs. Lacy,* 119 F3d 742, 9º Cir. 1997; *United States vs. Smith,* 47 MJ 588, CrimApp 1997; *United States vs. Ownby,* 926 FSupp 558, WDVa 1996.

13 Véase Julian Dibbell, «A Rape in Cyberspace», *Village Voice, op. cit.,* p. 36.

14 Las normas son algo diferente —regulando de forma más directa la conducta del usuario. Véase Daniel Benoliel, «Technological Standards, Inc.: Rethinking Cyberspace Regulative Epistemology», *California Law Review*, núm. 92, 2004, pp. 1069-1077.

Los mercados regulan la conducta en el ciberespacio. Las estructuras de precios restringen el acceso, y, si no, las señales de colapso de la red se encargan de hacerlo. (AOL aprendió esta lección de forma bastante drástica cuando pasó de un plan de cobro por horas a una tarifa plana).[15] Ciertas áreas de la red están comenzando a cobrar por acceder a ellas, tal y como hicieron durante algún tiempo los servicios *online*. Los anunciantes premian las páginas de éxito; los servicios *online* abandonan los foros de baja popularidad. Todas estas conductas están en función de las restricciones y oportunidades que ofrece el mercado, constituyendo, en este sentido, regulaciones de mercado.

Finalmente, un equivalente a la arquitectura regula la conducta en el ciberespacio —el código. El software y el hardware, que hacen del ciberespacio lo que es, constituyen un conjunto de restricciones sobre el modo en que podemos comportarnos en él. El contenido de dichas restricciones puede variar, pero éstas son experimentadas como condicionantes de nuestro acceso al ciberespacio. En algunos lugares (en servicios en red como AOL, por ejemplo), hemos de teclear una contraseña antes de acceder; en otros, podemos entrar con o sin identificación.[16] En algunos lugares, las transacciones que efectuamos producen rastros (los «clics de ratón») que permiten que nos asocien a dichas operaciones; en otros, esta asociación sólo se da si nosotros lo deseamos.[17] En algunos lugares, podemos elegir hablar una lengua que sólo el destinatario puede entender (mediante la criptografía);[18] en otros, esta opción está inhabilitada.[19] El código, o software, o arquitectura, o conjunto de protocolos establece estos atributos, seleccionados por los desarrolladores de código, que son, pues, los que posibilitan o imposibilitan determinadas conductas. El código lleva inscritos ciertos valores y hace imposibles otros y, en este sentido, constituye también un elemento de regulación, del mismo modo que la arquitectura en el espacio real.

---

15 Véase, por ejemplo, «AOL Still Suffering but Stock Price Rises», *Network Briefing,* 31 de enero de 1997; David S. Hilzenrath, «"Free" Enterprise, Online Style; AOL, CompuServe, and Prodigy Settle FTC Complaints», *Washington Post*, 2 de mayo de 1997, G1; «America Online Plans Better Information About Price Changes», *Wall Street Journal*, 29 de mayo de 1998, B2; véase también Swisher, *Aol.com*, *op. cit.,* pp. 206–8.

16 Los mensajes de USENET pueden ser anónimos; véase Henry Spencer y David Lawrence, *Managing USENET,* Sebastopol (Cal.), O'Reilly and Associates, 1998, pp. 366–367.

17 Los navegadores de Internet permiten disponer de esta información, tanto en tiempo real como en un archivo *cookie*; véase http://www.cookiecentral.com/faq.htm. Dichos navegadores también permiten a los usuarios desactivar este atributo de rastreo.

18 El PGP es un programa para cifrar mensajes que se ofrece tanto de forma comercial como gratuita.

19 El cifrado, por ejemplo, es ilegal en algunos contextos internacionales, véase Baker y Hurst, *The Limits of Trust, op. cit.*, pp. 130–136.

Tal y como sucede en el espacio real, pues, estas cuatro modalidades regulan el ciberespacio, a través de un equilibrio análogo al de aquél. William Mitchell lo expresa así (si bien omite la restricción derivada del mercado):

> La arquitectura, las leyes y las costumbres mantienen y representan todo equilibrio que se haya alcanzado en el espacio real. A medida que construimos y habitamos las comunidades del ciberespacio, tendremos que alcanzar y mantener pactos similares —por más que éstos se encarnen en estructuras de software y en controles de acceso electrónico más que en disposiciones arquitectónicas.[20]

Las leyes, las normas, el mercado y las arquitecturas interactúan para construir el entorno que conocen los «ciudadanos de la red» [*netizens*]. El desarrollador del código, tal y como afirma Ethan Katsh, es el «arquitecto».[21]

Ahora bien, ¿cómo podemos «alcanzar y mantener» este equilibrio entre modalidades de regulación? ¿De qué herramientas disponemos para conseguir una construcción diferente? ¿Cómo podría trasladarse al mundo del ciberespacio la combinación de principios del espacio real? ¿Cómo podría modificarse dicha combinación cuando así lo deseemos?

Sobre el Estado y las formas de regulación

Hasta aquí he descrito cuatro restricciones que afirmo que «regulan» a un individuo. Resulta obvio, no obstante, que cada una de estas restricciones no viene dada, simplemente, en la vida social, y que tampoco se encuentra en la naturaleza ni es dictada por Dios. Cada una de ellas puede modificarse, aunque los mecanismos para llevarlo a cabo entrañen no poca complejidad. La ley puede desempeñar un papel significativo en esta mecánica, y mi objetivo en esta sección es describir dicho papel.

Un ejemplo sencillo ayudará a exponer el argumento general que sostengo aquí. Digamos que el robo de radios de coche representa un problema —uno no demasiado grave en la escala de delitos, pero lo bastante frecuente y

---

20 Mitchell, *City of Bits*, *op. cit.*, p. 159.

21 Véase Ethan Katsh, «Software Worlds and the First Amendment», *op. cit.*, pp. 335-340: «Si fuera necesaria una comparación con el mundo físico, podría decirse que el desarrollador es el arquitecto, el constructor y el contratista, así como el decorador de interiores».

oneroso como para hacer necesaria una mayor regulación. Una posible respuesta sería elevar la pena por robar radios de coche hasta la cadena perpetua, de modo que el riesgo que afrontan los ladrones hiciese que no les mereciera la pena. Si los ladrones se dieran cuenta de que cada vez que roban una radio se exponen a cumplir cadena perpetua, puede que hacerlo dejara de tener sentido. La restricción que supone la amenaza de castigo por parte de la ley bastaría ahora para erradicar la conducta que tratamos de eliminar.

Ahora bien, la modificación de la ley no es la única técnica posible. Una segunda podría ser modificar la arquitectura de las radios de coche. Imaginémonos que los fabricantes de estas radios las programan de modo que sólo funcionen en un determinado coche —un código de seguridad que encadena electrónicamente la radio al coche, de modo que aquélla deje de funcionar si se la saca de éste. Ésta es una restricción del robo de radios efectuada mediante el código, el cual determina que, una vez robada, la radio ya no sirve para nada. Del mismo modo que la amenaza de cadena perpetua, esta restricción podría resultar efectiva para atajar la conducta del robo de radios.

Por lo tanto, la misma restricción puede lograrse a través de diferentes medios, y éstos conllevan distintos costes. La amenaza de cadena perpetua puede ser económicamente más gravosa que la modificación de la arquitectura de las radios (dependiendo de cuánta gente continúe robando radios y de cuántos de ellos sean atrapados). Desde esta perspectiva fiscal, puede resultar más eficaz modificar el código que cambiar la ley. La eficacia fiscal puede ponerse del lado del contenido expreso de la ley —sería una barbaridad aplicar una pena tan extrema a un delito tan leve. Así pues, los principios pueden respaldar la respuesta más eficaz, de forma que el código resultaría el mejor medio de regulación en este caso.

Los costes, sin embargo, no siempre se ponen del lado de los principios. Tomemos el ejemplo hipotético de que el Tribunal Supremo dictamine la imposición de cadena perpetua a quienes no paguen el ticket de aparcamiento.[22] Es probable que cualquier restricción impuesta por el código, por más práctica que fuera, nunca superara en eficacia a la restricción legal (asumiendo que el único objetivo fuera la reducción de las infracciones de aparcamiento). Lo cierto es que serían muy escasas las víctimas que se cobrara esta ley antes de que la gente conformara su conducta a ella adecuadamente. Con todo, el «resultado eficaz» entraría en conflicto con otros principios. Si resulta una barbaridad encarcelar a alguien de por vida por robar una

---

22 Véase *Rummel vs. Estelle,* 445 US 263, 274, núm. 11, 1980.

radio, más barbaridad aún es hacerlo por una infracción de aparcamiento. El regulador dispone de un repertorio de medios para efectuar la restricción deseada, pero los principios que dichos medios comportan no necesariamente coinciden con su eficacia. La respuesta más eficaz puede muy bien resultar injusta —esto es, puede entrar en conflicto con los principios inherentes a las normas, o a la ley (la Constitución), de la sociedad.

Resulta típico del discurso jurídico ignorar estos otros tres reguladores y cómo la ley puede influir sobre la regulación que efectúan. Muchos juristas hablan como si la ley simplemente debiera dar por sentadas las otras tres restricciones y adaptarse a ellas.[23]

Y digo «como si» porque hoy basta reflexionar un segundo para ver que tal estrechez de miras es absurda. Hubo épocas en que estas otras restricciones eran tratadas como fijas —épocas en que se decía que las restricciones normativas eran inamovibles por la acción del Estado,[24] o en que se concebía el mercado como esencialmente irregulable,[25] o en que el coste de modificar el código del espacio real era tan elevado que se desestimaba por absurdo su uso para la regulación.[26] En la actualidad, en cambio, comprobamos que estas restricciones poseen un carácter plástico,[27] que son, al igual que la ley, modificables y susceptibles de regulación.

---

23 Resulta interesante —y es de nuevo una razón para ver situado en otra parte el futuro de la discusión sobre la regulación— comprobar que esto no es cierto con respecto a los arquitectos. Un ejemplo de ello lo constituye la obra de John de Monchaux y J. Mark Schuster. En su ensayo «Five Things to Do» y en la colección de textos que dicho ensayo presenta, *Preserving the Built Heritage*, *op. cit.*, estos autores describen las «cinco y nada más que cinco cosas que los Estados pueden hacer —cinco herramientas distintas que pueden utilizar— para implementar sus políticas», pp. 4–5: propiedad y operación (el Estado puede poseer el recurso), regulación (tanto de los individuos como de las instituciones), incentivos, derechos de propiedad e información. Las cinco herramientas de Monchaux y Schuster mapean de forma compleja la estructura que he descrito, pero compartimos significativamente una concepción de la regulación como una constante negociación entre herramientas.

24 Véase, por ejemplo, James C. Carter, *The Provinces of the Written and the Unwritten Law*, Nueva York, Banks and Brothers, 1889, donde el autor arguye que es imposible cambiar el derecho consuetudinario (pp. 38–41).

25 Véase, por ejemplo, la discusión en torno a la teoría del fondo de salarios en Hovenkamp, *Enterprise and American Law*, *op. cit.*, pp. 193–196.

26 Para un relato fascinante de la maduración de la idea de que el entorno natural podría domesticarse con un propósito productivo e industrializado, véase John M. Barry, *Rising Tide: The Great Mississippi Flood of 1927 and How It Changed America*, Nueva York, Simon and Schuster, 1997.

27 Tal y como lo expresa Roberto Unger: «El pensamiento social moderno nació proclamando que la sociedad es construida e imaginada, que constituye un artefacto humano más que la expresión de un orden natural subyacente»; *Social Theory Politics: A Work in Constructive Social Theory,* v. II, Nueva York, Cambridge University Press, 1987, p. 1.

Los ejemplos son tan obvios como abundantes. Pensemos, en primer lugar, en el mercado: a pesar de la monserga sobre el «libre mercado», no existe un ámbito de nuestra vida más regulado que éste.[28] El mercado está regulado por la ley, no sólo en sus elementos —es la ley la que hace cumplir los contratos, establece la propiedad y regula la moneda—, sino también en sus efectos. La ley usa los impuestos para incrementar la restricción que el mercado ejerce sobre ciertas conductas, y las subvenciones para reducir la que ejerce sobre otras. Gravamos los cigarrillos para reducir su consumo, pero subvencionamos la producción tabaquera para incrementar su oferta. Gravamos el alcohol para reducir su consumo y subvencionamos la educación infantil para reducir las limitaciones que el mercado impone sobre la crianza de los niños. De éstas y otras muchas formas, la restricción legal se emplea para modificar las restricciones del mercado.

La ley también puede modificar la regulación arquitectónica. Pensemos en la ADA (*Americans with Disabilities Act*, Ley de los estadounidenses con discapacidades).[29] Muchas personas con «discapacidades» quedan relegadas del acceso a gran parte del mundo. Un edificio equipado únicamente con escaleras resulta inaccesible para una persona en silla de ruedas; las escaleras suponen una restricción para el acceso de esa persona al edificio. El objetivo de la ADA, al menos en parte, es transformar esa restricción exigiendo que los constructores cambien el diseño de sus edificios de modo que las personas con discapacidad motriz no queden excluidas de ellos. He aquí una regulación legal del código del espacio real cuya finalidad es transformar la restricción que genera dicho código.

Otros ejemplos son aún mejores:

– Parte del potencial de la Revolución Francesa derivó de la arquitectura de la ciudad de París: sus calles pequeñas y sinuosas facilitaban el levantamiento de barricadas, lo que permitió a los revolucionarios hacerse con el control de la ciudad desplegando una fuerza absoluta relativamente reducida. Luis Napoleón III comprendió esto posteriormente y, en 1853, tomó las medidas necesarias para transformar la arquitectura parisina.[30]

---

28 La idea de un mercado libre obsesionaba a los realistas, especialmente a Robert Hale; véase Barbara H. Fried, *The Progressive Assault on Laissez-Faire: Robert Hale and the First Law and Economics Movement*, Cambridge (Mass.), Harvard University Press, 1998: «La vida económica, igual que el mercado moral de Clark, estaba constituida por un régimen de propiedad y derechos contractuales que no era ni espontáneo ni autodefinitorio, sino más bien una creación positiva del Estado», pp. 2–3. Para una revisión moderna de esto, véase Cass R. Sunstein, *The Partial Constitution*, Cambridge (Mass.), Harvard University Press, 1993, pp. 51–53.

29 *Americans with Disabilities Act* (ADA) de 1990, 42 USC, Secciones 12101 *et seq*., 1994.

30 Véase Alain Plessis, *The Rise and Fall of the Second Empire, 1852–1871*, Nueva York, Cambridge University Press, 1985, p. 121; «Haussmann, Baron Georges-Eugène», en *Encyclopedia Britannica*, (5ª),

París fue reconstruida sobre la base de amplios bulevares y múltiples pasajes para imposibilitar que otros insurgentes tomaran de nuevo la ciudad.

– Todos los escolares estadounidenses aprenden el diseño elaborado por el arquitecto L'Enfant para dificultar una hipotética invasión de Washington. Más interesante aún resulta el emplazamiento que, en dicha capital, recibió la Casa Blanca con respecto al Capitolio (sede del Congreso). La distancia entre ambos edificios es de una milla, y antaño, se trataba de una milla de terreno accidentado (el National Mall, parque construido en esta área a principios del siglo XX, era por entonces una ciénaga). Tal distancia constituía, así, una barrera que, obstaculizando la conexión entre el Congreso y el Presidente, dificultaba sus relaciones y, de resultas, el control del poder legislativo por parte del poder ejecutivo.

– Esta misma idea ha influido en el emplazamiento de los Tribunales Constitucionales en Europa, que se colocaron en ciudades distintas a la capital del país. En Alemania, la sede del Tribunal Constitucional se fijó en Karlsruhe en lugar de en Berlín; en la República Checa, está situada en Brno en lugar de en Praga. De nuevo, el motivo viene asociado a una restricción de naturaleza geográfica: situando el Tribunal Constitucional en un lugar apartado de la sede de los poderes legislativo y ejecutivo se buscaba tanto minimizar la presión que éstos pudieran ejercer sobre aquél como reducir su tentación de plegarse a dicha presión.

– Este principio no se limita a la alta política. Los diseñadores de aparcamientos o de calles donde pueden jugar niños colocan badenes para que los conductores disminuyan la velocidad. Estas estructuras tienen el mismo propósito que la imposición legal de un límite de velocidad o que una norma contra el exceso de velocidad, pero operan modificando la arquitectura.

– Tampoco se limita a la regulación virtuosa; Robert Moses construyó puentes en la isla estadounidense de Long Island para bloquear su acceso en autobús, de modo que los ciudadanos afroamericanos, que dependían fundamentalmente del transporte público, no pudieran llegar fácilmente a las playas públicas.[31] Éste es un caso claro de regulación mediante la arquitectura, abominable, pero que nos resulta familiar.

1992. Steven Johnson critica otros aspectos de esta transformación en *Interface Culture*, op. cit., pp. 63–64. [Sobre este tema, en castellano: David Harvey, *París, capital de la modernidad*, trad. por José María Amoroto Salido, Madrid, Ed. Akal, 2008. N del E.]

31 Véase Robert A. Caro, *The Power Broker: Robert Moses and the Fall of New York*, Nueva York, Alfred A. Knopf, 1974, p. 318.

– Y tampoco se limita a los Estados. Una importante compañía aérea estadounidense se percató de que los pasajeros de los vuelos de los lunes a primera hora se mostraban enojados por el tiempo de espera para recoger su equipaje. Lo cierto es que este tiempo no era superior al tiempo medio de espera, pero estos pasajeros se mostraban mucho más enfadados que los de otros vuelos. La compañía comenzó a aparcar estos vuelos en puertas más alejadas de la zona de recogida de equipajes, de modo que para cuando los pasajeros llegaban a ella, sus maletas ya estaban allí. Así se eliminó la frustración con respecto al sistema de tratamiento de equipaje.

– Un gran hotel de una ciudad estadounidense recibió muchas quejas por la lentitud de sus ascensores. Tras instalar espejos en las puertas de los ascensores, las quejas cesaron.

– Es probable que pocos conozcan al partidario más destacado de la regulación mediante la arquitectura del siglo XX —Ralph Nader. Resulta asombroso leer hoy el relato de su batalla para conseguir que se exigiera que los fabricantes de automóviles cumplieran con los estándares de seguridad. El objetivo primordial de Nader consistía en lograr que la ley obligara a dichos fabricantes a construir coches más seguros. En la actualidad es obvio que el código de los coches es una parte esencial de la seguridad automovilística, pero esta idea básica generó una profunda controversia hace unas décadas.[32]

– Neal Katyal ha analizado extensamente la relación entre la arquitectura y las leyes criminales, desde la instalación del alumbrado en las calles hasta el diseño de espacios públicos para maximizar la visibilidad.[33] Así, por ejemplo, los Juegos Olímpicos de Sidney 2000 «recurrieron conscientemente a la arquitectura para reducir los crímenes».[34] Y los arquitectos han comenzado a identificar principios de diseño capaces de reducir los crímenes —lo que se denomina «prevención del crimen mediante el diseño del entorno».[35]

En cada uno de estos ejemplos observamos que se modifica la arquitectura para dar lugar a una conducta diferente. Es la arquitectura la que marca esa diferencia. Como se leía en un letrero situado sobre una de las

---

32 Ralph Nader, *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*, Nueva York, Grossman, 1965, p. xciii.

33 Véase Neal Kumar Katyal, «Architecture as Crime Control», *Yale Law Journal*, núm. 111, pp. 1039, 2002.

34 *Ibidem*, p. 1047.

35 *Ibidem*, p. 1048.

puertas de entrada a la Exposición Universal de Chicago de 1933 (aunque el letrero aludía a la ciencia): «La ciencia explora; la tecnología ejecuta; el hombre se conforma».[36]

La ley también puede cambiar las normas sociales, por más que buena parte de nuestra jurisprudencia constitucional se empeñe en que olvidemos cómo se hace.[37] La educación es el ejemplo más obvio. Como afirma Thurgood Marshall: «La educación no consiste en enseñar el "abc" de los conocimientos, sino en enseñar las bases de la ciudadanía, consiste en aprender a convivir con nuestros conciudadanos y, por encima de todo, en aprender a obedecer la ley».[38] La educación es, al menos en parte, un proceso por el cual adoctrinamos a los niños en ciertas normas de conducta —les enseñamos a «decir no» al sexo y las drogas. De esta manera, tratamos de infundirles un sentido de lo que es correcto, sentido que les regula entonces según el objetivo de la ley.

Dicho claramente, el contenido de buena parte de la educación viene regulado por la ley. A los conservadores les inquieta, por ejemplo, que por impartir a los niños la asignatura de educación sexual podamos cambiar la norma de la abstinencia sexual. Sea cierto o no, se está usando la ley para

---

36 Brin, *The Transparent Society*, *op. cit.*, p. 293.

37 Tomemos en consideración los derechos civiles en el sur de EEUU. Durante las vistas legislativas sobre la *Civil Rights Act* (la Ley de Derechos Civiles) de 1964, los defensores de esta propuesta llamaron a declarar ante el tribunal a empleadores y propietarios de negocios blancos y sureños, cuya discriminación contra los negros era el principal objeto de la legislación. Algunos de ellos respaldaron la ley porque sus negocios mejorarían con ella: el mercado de trabajo se incrementaría, provocando un descenso de los salarios y un aumento de la demanda de servicios —siempre, eso sí, que los blancos no cambiaran sus costumbres. Fue este último aspecto el que dio pie al apoyo empresarial a la Ley de Derechos Civiles. Lo que temían los dueños de negocios eran las represalias de los blancos contra sus esfuerzos voluntarios de integración, y la Ley de Derechos Civiles modificó el contexto para ilegalizar la discriminación contra los negros. A partir de ese momento, los hombres de negocios podían —sin temor a las represalias de los blancos— contratar o poner a su servicio a negros, ya fuera por su concienciación con respecto a la situación social de éstos o por su preocupación por obedecer la ley. Al generar esta ambigüedad, la ley reducía los costes simbólicos que acarreaba contratar a negros. Este ejemplo demuestra cómo la ley puede cambiar las normas sin que el Estado tenga que ejercer ningún control sobre ellas. En este caso, la norma de integrar a los negros se modificó al agregarle un segundo significado —la norma de limitarse a obedecer la ley; véase Lessig, «The Regulation of Social Meaning», *The University of Chicago Law Review*, vol. 62, núm. 3, 1995, pp. 965–67.

38 Thurgood Marshall, Esq., argumentación oral de parte de los demandados, *Cooper vs. Aaron*, 358 US 1, 1958, núm. 1, en Philip B. Kurland y Gerhard Casper (eds.), *Fifty-four Landmark Briefs and Arguments of the Supreme Court of the United States: Constitutional Law*, Washington DC, University Publications of America, 1975, pp. 533, 713.

modificar las normas de los niños. Si los conservadores tienen razón, la ley está eliminando la abstinencia; si son los progresistas quienes están en lo cierto, la ley está usándose para inculcar a los niños una norma de sexo seguro. Sea como fuere, las normas disponen de su propia capacidad restrictiva, y la ley está tratando de cambiar dicha restricción.

Afirmar que la ley desempeña un papel no implica afirmar que éste siempre sea positivo. La ley puede echar a perder normas del mismo modo que puede mejorarlas, y aquí no estoy defendiendo que esto último sea lo más frecuente.[39] Lo que me interesa aquí es comprender este papel, no alabarlo o criticarlo.

En cada caso, la ley escoge entre la regulación directa y la indirecta. La pregunta es: ¿qué medios contribuyen mejor al objetivo del regulador, asumiendo las restricciones (sean normativas o materiales) que éste debe reconocer? Mi argumento es que el análisis de las estrategias de regulación ha de tener en cuenta estas diferentes modalidades. Polk Wagner lo expresa así, centrándose en una modalidad adicional:

> Del mismo modo que la elección de una regla legal implicará negociaciones analíticas entre las conocidas categorías de reglas de propiedad y reglas de responsabilidad, la incorporación de reglas de prelación legal en el contexto del ciberespacio requerirá un ejercicio parecido en una dimensión adicional —el impacto que la regla legal tendrá en la regulación de software correspondiente (y, por lo tanto, su efecto en la interfaz ley-software).[40]

En caso contrario, de nuevo, «las propuestas legales de políticas públicas que no tengan en cuenta la respuesta tecnológica resultan profundamente incompletas».[41] Y lo mismo puede afirmarse de forma general acerca de la interacción entre cualquiera de las modalidades y cualquier legislación.

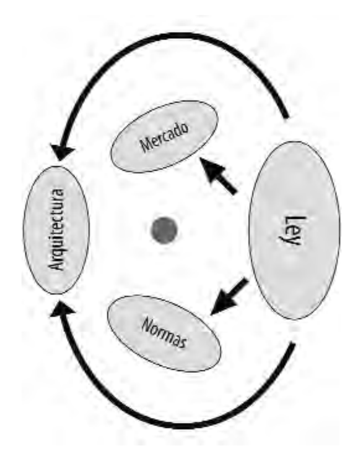
Podemos representar este argumento a través de una modificación de la figura anterior:

---

39 Véase, por ejemplo, Dyson, *Release 2.0*: «El Estado puede desempeñar un papel fragmentador de cara a las comunidades. A menudo, cuanto más aporta el Estado, menos contribuyen los miembros de la comunidad», *op. cit.*, p. 43; en «The Regulation of Groups: The Influence of Legal and Nonlegal Sanctions on Collective Action», *University of Chicago Law Review*, núm. 63, 1996, p. 133, Eric A. Posner sostiene que la ayuda estatal a una comunidad puede contribuir a socavar dicha comunidad.

40 R. Polk Wagner, «On Software Regulation», *Southern California Law Review*, núm. 78, 2005, pp. 457-487.

41 *Ibidem*, p. 474.



Tal y como recalca acertadamente Wagner, una vez más, la interacción entre estas modalidades es dinámica, «exigiendo no sólo tomar en consideración [...] las modificaciones legales, sino también predecir los efectos prácticos que tales cambios estimularán».[42] Así, el regulador intenta alcanzar un «equilibrio» considerando constantemente las negociaciones entre las distintas modalidades de regulación.

El argumento debería resultarnos ya familiar, y los ejemplos pueden ser múltiples.

– *Cinturones de seguridad*: el Estado puede querer que sus ciudadanos utilicen el cinturón de seguridad más a menudo.[43] En este sentido, podría promulgar una ley que exija su uso a los conductores (la ley regulando directamente la conducta). O bien podría financiar campañas educativas públicas destinadas a estigmatizar a aquéllos que no usen el cinturón (la ley regulando las normas sociales como un medio para regular la conducta). O bien podría subvencionar a las compañías aseguradoras para que ofrecieran

42 *Ibidem*, p. 465.

43 Cass Sunstein señala la ley aplicada a los cinturones de seguridad como una hipotética «regulación estatal que permite que la gente exprese sus preferencias escudándose en la ley para disminuir el riesgo de que los actores privados interfieran en la expresión [mediante la censura normativa]»; «Legal Interference with Private Preferences», *University of Chicago Law Review*, núm. 53, 1986, pp. 1129, 1145. De modo alternativo, las leyes relativas a los cinturones de seguridad han sido usadas como la base factual para criticar el patrocinio de las normas como ineficaz y no susceptible de sustituir a la regulación directa; véase Robert S. Alder y R. David Pittle, «Cajolery or Command: Are Education Campaigns an Adequate Substitute for Regulation?», *Yale Journal on Regulation*, núm. 1, 1984, pp. 159, 171–178. No obstante, puede que estas observaciones hayan sido prematuras. John C. Wright, en su comentario sobre el contenido normativo de la televisión, sostiene que «hemos ganado la batalla de los cinturones de seguridad sólo porque un puñado de personas se han unido para decir: "Es de lo más masculino ponerse el cinturón de seguridad. Es de machos, inteligente y varonil, y también es femenino e inteligente, sagaz y encantador ponerse el cinturón de seguridad"»; Charles W. Gusewelle *et al.*, «Round Table Discussion: Violence in the Media», *Kansas Journal of Law and Public Policy,* núm. 4, 1995, pp. 39, 47.

tarifas reducidas a quienes usaran el cinturón (la ley regulando el mercado como una vía de regular la conducta). Finalmente, la ley podría ordenar la instalación de cinturones de seguridad automáticos, o bien de sistemas de bloqueo de arranque (modificando el código del automóvil como un medio de regular la conducta de uso de los cinturones). Puede afirmarse que cada una de estas acciones provocará un cierto efecto sobre el uso del cinturón de seguridad, y también que entrañará un cierto coste. La cuestión que se le plantea al Estado es, pues, cómo conseguir el uso más amplio del cinturón de seguridad al menor coste.

– *Discriminación contra las personas con discapacidad*: en su vida cotidiana, las personas con discapacidad soportan barreras significativas de orden social y físico.[44] El Estado podría decidir hacer algo con respecto a dichas barreras. La respuesta tradicional consiste en que la ley regule la conducta de forma directa: una ley que prohíba la discriminación basada en la discapacidad física. Ahora bien, hay algo más que la ley podría hacer. Por ejemplo, podría educar a los niños con el fin de cambiar las normas sociales (regulando las normas para regular la conducta). También podría subvencionar a las compañías para contratar a personas con discapacidad (regulando el mercado para regular la conducta). Finalmente, podría regular los códigos de edificación para que los edificios resultasen más accesibles para dichas personas (regulando los códigos «naturales» o del espacio real para regular la conducta). Cada una de estas regulaciones provocaría un cierto efecto sobre la discriminación, y entrañaría asimismo un cierto coste. El Estado tendría que sopesar los costes y los beneficios para seleccionar el modo de regulación más efectivo.

– *Drogas*: el Estado está obsesionado con reducir el consumo de drogas ilícitas. Hasta ahora, su estrategia principal ha sido la regulación directa de la conducta a través de la amenaza de penas de prisión desaforadas a quienes violen las leyes antidroga. Esta política implica unos costes muy obvios y unos beneficios que no lo son tanto, siendo estos últimos los que más nos interesan para nuestros propósitos. Tal y como argumenta de modo persuasivo Tracey Meares, una estructura social eficaz para regular el consumo de drogas ilegales es la de la comunidad donde vive un individuo.[45] Esto es lo que yo he denominado

---

44 Este análisis vino sugerido, en parte, por la obra de Minow, *Making All the Difference*, *op. cit*.

45 Véase Tracey L. Meares, «Social Organization and Drug Law Enforcement», *American Criminal Law Review*, núm. 35, 1998, p. 191.

restricciones derivadas de las normas sociales: patrones de comportamiento adecuado sancionados por una comunidad —ya sea por medio de la vergüenza, la exclusión o la fuerza.

Del mismo modo que el Estado puede actuar para reforzar estas restricciones derivadas de las normas sociales, es obvio que también puede hacerlo para debilitarlas.[46] Un modo de lograr esto es debilitando las propias comunidades en las que operan dichas normas. Esto, afirma Meares, es lo que están consiguiendo las excesivas sanciones previstas en el código penal.[47] Por su extremismo y por las consecuencias que acarrean, dichas sanciones socavan las estructuras sociales que respaldarían esas políticas sociales. Éste es un efecto indirecto de la regulación directa de la ley que, llegado a un cierto punto, puede llegar a superar el efecto de la ley. Es lo que podríamos llamar la Curva Laffer del Código Penal.

El efecto combinado de estas diferentes restricciones no puede deducirse a priori. El Estado actúa de muchas formas para regular el consumo de drogas. Así, por una parte, apoya amplias campañas de educación pública destinadas a estigmatizar el consumo de drogas (regulando las normas sociales para regular la conducta). Incauta alijos de droga a su paso por la frontera, disminuyendo de este modo el suministro, incrementando los precios y, supuestamente, reduciendo la demanda (regulando el mercado para regular la conducta). A veces incluso ha regulado (de manera esperpéntica) el «código» de las drogas con el fin de hacerlas más peligrosas y, de esta manera, incrementar las restricciones sobre su consumo, por ejemplo, rociando las plantaciones de marihuana con paraquat.[48] Todo esto, en su conjunto, influye en el consumo de drogas pero, como argumentan los partidarios de su

---

46 En «The Regulation of Groups», *op. cit.,* Eric Posner señala ciertos contextos en los que la acción del Estado puede haber provocado este efecto.

47 Véase Tracey L. Meares, «Charting Race and Class Differences in Attitudes Toward Drug Legalization and Law Enforcement: Lessons for Federal Criminal Law», *Buffalo Criminal Law Review*, núm. 1, 1997, p. 137.

48 A mediados de la década de los setenta, el gobierno estadounidense impulsó una campaña para rociar de paraquat (un herbicida que causa daños pulmonares a los humanos) las cosechas de marihuana de México. Esto desencadenó una protesta popular que trajo como resultado la suspensión de la financiación del Congreso en 1978. Sin embargo, tras una enmienda aprobada en el Congreso en 1981, el paraquat volvió a utilizarse durante los años ochenta para rociar las cosechas de marihuana nacionales. Se cree que la publicidad que rodeó el uso de paraquat en México provocó el auge de la industria interior de marihuana, incrementando de paso la popularidad de la cocaína durante la década de los ochenta. Véase, en general, Michael Isikoff, «DEA Finds Herbicides in Marijuana Samples», *Washington Post*, 26 de julio de 1989, p. 17. En «Drug Diplomacy and the Supply-

legalización, también influye en la incidencia de otras conductas criminales. Los diseñadores de las políticas antidroga deben realizar una estimación del efecto combinado de sus decisiones —esto es, si, en conjunto, estas regulaciones reducen o incrementan los costes sociales.

– *Aborto*: un ejemplo final servirá para completar esta lista. A partir del caso «Roe contra Wade», el Tribunal Supremo ha reconocido el derecho constitucional a abortar que asiste a las mujeres estadounidenses.[49] Con todo, este reconocimiento no ha servido para detener al Estado en su intento de eliminar o reducir el número de abortos en EEUU. Una vez más comprobamos que el Estado no necesita recurrir a la regulación directa contra el aborto (lo cual, en virtud del caso citado, sería inconstitucional), sino que, en lugar de eso, puede emplear medios indirectos para lograr sus fines. En el caso «Rust contra Sullivan», el Tribunal Supremo ratificó el poder del Estado para influir en las asesorías de planificación familiar, mediante la prohibición a los médicos que trabajaban en clínicas «financiadas por el Estado» de mencionar el aborto como un método de planificación familiar.[50] Ésta es una regulación de las normas sociales (en el seno de la estructura social de la asistencia sanitaria) para regular la conducta. En el caso «Maher contra Roe», el Tribunal Supremo ratificó el derecho del Estado a retirar selectivamente la financiación médica para llevar a cabo abortos.[51] Estamos ante el uso del mercado para regular la conducta. Y en el caso «Hodgson contra Minnesota», el Tribunal Supremo ratificó el derecho del Estado a obligar a las mujeres menores de edad a esperar cuarenta y ocho horas para someterse a un aborto que hubieran solicitado.[52] Estamos ante el uso del código del espacio real (las restricciones impuestas por el tiempo) para regular el acceso al aborto. Por todos estos medios, y a pesar de la sentencia del caso «Roe contra Wade», el Estado puede regular la conducta de las mujeres que desean abortar.

En cada uno de estos ejemplos, la ley funciona de dos formas muy diferentes.[53] Cuando opera directamente, dicta a los individuos cómo han de comportarse y amenaza con castigos si se desvían de sus directrices; cuando

---

Side Strategy: A Survey of United States Practice», *Vanderbilt Law Review*, núm. 43, 1990, pp. 1259-1275, Sandi R. Murphy traza una historia detallada de las leyes que se promulgaron con respecto al paraquat; véase también «A Cure Worse Than the Disease?», *Time*, 29 de agosto de 1983, p. 20.

49 *Roe vs. Wade,* 410 US 113, 1973.

50 *Rust vs. Sullivan*, 500 US 173, 1991.

51 *Maher vs. Roe,* 432 US 464, 1977.

52 *Hodgson vs. Minnesota,* 497 US 417, 1990.

53 Esta distinción entre regulación «directa» e «indirecta» tiene, por supuesto, una historia dilatada y azarosa tanto en el ámbito filosófico como en el jurídico. Judith J. Thomson describe esta

opera indirectamente, modifica una de las otras estructuras de restricción.[54] El regulador elige entre estas distintas técnicas en función de lo que espera de ellas —tanto en términos de eficacia como según los principios que cada una sustenta.

Cuando observamos la regulación de este modo más general, podemos percibir más claramente cómo la irregulabilidad del ciberespacio es contingente. De esta manera, adquirimos una sólida conciencia acerca de cómo el Estado podría intervenir para hacer funcionar la regulación y, también, acerca de los peligros crecientes que implica este sentido más expansivo de la regulación. Más concretamente, acerca del peligro que esto representa con respecto a los valores constitucionales. La próxima sección está dedicada a examinar una de estas amenazas.

Los problemas de la regulación indirecta

En 1985, y tras varios años de pasividad en este ámbito, el Congreso promulgó la *Low Level Radioactive Waste Policy Amendments Act* (Ley de Enmiendas sobre la Política de Residuos Radioactivos de Baja

diferencia en su distinción entre el conductor de tranvía que ha de atropellar a una persona para salvar a cinco, y el cirujano que no puede extraer a una persona sana sus órganos para salvar a cinco personas moribundas; véase «The Trolley Problem», *Yale Law Journal*, núm. 94, 1985, pp. 1395–1396. A esta diferencia se la conoce también como la «doctrina del doble efecto», discutida en Philippa Foot, «The Problem of Abortion and the Doctrine of the Double Effect», en *Virtues and Vices and Other Essays in Moral Philosophy*, Berkeley, University of California Press, 1978, p. 19 [ed. cast.: *Las virtudes y los vicios y otros ensayos de filosofía moral*, trad. por Claudia Martínez, IIFs-UNAM, México, 1994]. Véase también Thomas J. Bole III, «The Doctrine of Double Effect: Its Philosophical Viability», *Southwest Philosophy Review*, núm. 7, 1991, p. 91; Frances M. Kamm, «The Doctrine of Double Effect: Reflections on Theoretical and Practical Issues», *Journal of Medicine and Philosophy*, núm. 16, 1991, p. 571; Warren Quinn, «Actions, Intentions, and Consequences: The Doctrine of Double Effect», *Philosophy and Public Affairs*, núm. 18, 1989, p. 334. En estos casos el problema surge cuando ha de trazarse una línea de separación entre ellas, lo que no ocurre en nuestra reflexión.

54 Richard Craswell sugiere otros ejemplos que ilustran este mismo argumento: el Estado podría a) regular la calidad o seguridad de los productos, o b) desvelar información acerca de los índices de calidad o seguridad de distintos productos, con la esperanza de que los fabricantes tendrían entonces un incentivo para competir de cara a la mejora de esos índices; el Estado podría a) permitir que una industria permanezca monopolizada e intentar regular de forma directa el precio que impone dicho monopolio, o b) dividir la empresa monopolística en varias compañías que compitan entre sí, con la esperanza de que esta situación las obligue a fijar precios más competitivos; el Estado podría a) promulgar regulaciones que exijan directamente a las empresas realizar acciones en beneficio del interés público, o b) promulgar regulaciones que exijan a las empresas que incluyan en sus juntas directivas un cierto número de representantes «independientes», con la esperanza de que dichas juntas decidan por sí mismas actuar de forma más coherente con el interés público.

Intensidad) para abordar el problema de los residuos nucleares, ya que resultaba necesario que alguien los recogiera y almacenase.[55] Después de que el gobierno ejerciera la pertinente presión, varios Estados alcanzaron un pacto, que fue ratificado por el Congreso, por el cual se implementarían una serie de requisitos y de incentivos para que los Estados tratasen los residuos nucleares que produjeran.

Los detalles generales del plan no revisten importancia para nuestra finalidad aquí, por lo que nos concentraremos en uno solo de sus aspectos. Con el fin de inducir a los Estados a seguir las directrices federales de regulación de residuos nucleares, el Congreso les planteó la siguiente opción: o bien promulgaban ciertas regulaciones al respecto, o bien «asumían la titularidad» de los desechos de combustible nuclear. Se trataba de una regulación del tipo «la bolsa o la vida», puesto que la titularidad de los desechos no reportaba a los Estados ningún activo, sino más bien una enorme responsabilidad. Aplicando toda su mano dura, el Congreso estaba obligando, en esencia, a que los Estados aprobaran la regulación que él imponía.

El Tribunal Supremo derogó esta parte de la ley, alegando que, en efecto, el Congreso estaba invadiendo las competencias legislativas de los Estados para imponerles su ley. Por supuesto, el Congreso disponía por sí mismo del poder para promulgar directamente dicha regulación, pero no para ordenar que los Estados la aprobaran. En esta ocasión, no se le consintió al gobierno federal regular de manera indirecta.

Este caso —«El Estado de Nueva York contra Estados Unidos»— no manifiesta que el Estado deba regular únicamente de modo directo, y tampoco que la regulación indirecta se vea generalmente desfavorecida. El caso se redujo estrechamente a la cuestión de «regular de manera indirecta» con respecto a los Estados, centrándose en la defensa de la idea de que los Estados, como instancias soberanas e independientes que merecen un respeto constitucional especial, no pueden sufrir injerencias por parte del gobierno federal —que, cuando desee implementar un programa propio, debe hacerlo de forma explícita.

Ahora bien, por más que este caso no establezca un principio constitucional de carácter general, sí que sugiere por qué la regulación indirecta debería suscitar una mayor preocupación.

---

55 Véase *New York vs. United States*, 505 US 144, 1992.

La regulación indirecta desvía la responsabilidad. Cuando un Estado emplea otras estructuras de restricción para ejercer una restricción que podría imponer de modo directo, enturbia la responsabilidad sobre dicha restricción y, de esta manera, socava el proceso de rendición política de cuentas. Si la transparencia constituye uno de los principios de un Estado constitucional, la regulación indirecta es su enemiga, puesto que confunde la responsabilidad y, por ende, la política.[56]

Tales malentendidos también pueden darse en otros contextos. Volvamos de nuevo al caso. El gobierno federal contribuye a financiar las clínicas de planificación familiar («contribuye» a financiar, no financia completamente).[57] Antes de 1988, estas clínicas proporcionaban asesoramiento sobre un amplio abanico de temas relacionados con la concepción, incluyendo el aborto. Así, los médicos de estas clínicas aconsejaban a sus pacientes recurrir al aborto cuando lo consideraban la opción más apropiada para ellas.

La Administración Reagan quería cambiar esta situación, así que ordenó (los detalles tampoco revisten mayor importancia en este caso) a los médicos de esas clínicas no discutir con sus pacientes acerca del aborto como método de planificación familiar. En caso de que se les consultara a ese respecto, debían responder: «Nuestro programa no considera el aborto un método de planificación familiar adecuado».[58]

El propósito de esta regulación era bien claro: reducir la incidencia del aborto. Para alcanzarlo, el Estado utilizó a los médicos con el fin de disuadir a las pacientes de abortar. Un médico ostenta un amplio grado de poder sobre una paciente en un contexto como éste, y lo más probable es que dicha paciente creyera que el médico de verdad le estaba desaconsejando el aborto.

---

56 Lee Tien identifica otros problemas importantes relativos a la regulación arquitectónica en «Architectural Regulation and the Evolution of Social Norms», *International Journal of Communications Law and Policy*, núm. 9, 2004, p. 1.

57 Aida Torres, «The Effects of Federal Funding Cuts on Family Planning Services, 1980–1983», *Family Planning Perspectives*, núm. 16, 1984, pp. 134-136.

58 *Rust vs. Sullivan*, USNY, 1990, WL 505726, informe de respuestas, *7: «El médico no puede explicar la seguridad médica del procedimiento, su disponibilidad legal o su importancia acuciante para la salud de la paciente».

Pero fijémonos en la técnica empleada. El gobierno federal podría haber declarado públicamente su postura contra el aborto, exponiendo en carteles y vallas publicitarias que el aborto es perjudicial, o bien publicitando esta idea en las propias clínicas. Sin embargo, en lugar de ello, optó por camuflar su opción política bajo capa de discurso médico. De esta forma, podría sacar partido de la autoridad profesional de los médicos para promover sus propios fines, regulando indirectamente el aborto mediante la regulación directa de los médicos.

Del mismo modo que antes trató de usar la autoridad de los Estados para alcanzar sus propios fines, en el caso «Rust contra Sullivan», la administración federal se aprovecha de la distorsión en las declaraciones médicas. Ahora bien, aquí sucede algo más grave que en el contexto del federalismo, y es que la víctima de dicha distorsión ni siquiera se percata de que detrás de ella se esconde una opción política. Es muy improbable que la paciente interprete los consejos de su médico de la misma forma que escucha un discurso político gubernamental; lo más probable es que los interprete como una opinión médica. Por consiguiente, no sólo se genera una confusión acerca de quién es responsable de la opinión expresada, sino también acerca de si se trata siquiera de *una opinión*.

El caso «Rust contra Sullivan» es uno de los más embarazosos a los que se haya enfrentado el Tribunal Supremo —probando, de paso, la regla del juez Scalia según la cual cualquier asunto queda distorsionado desde el momento en que se aproxima al tema del aborto.[59] Sea como fuere, el argumento que defiendo aquí no depende de si esta sentencia fue más o menos afortunada, mi objetivo es destacar una cierta sensibilidad acerca de la regulación: el caso «Rust contra Sullivan» simplemente nos señala el camino.

Examinemos un tercer caso. En EEUU, hasta el año 1948, las escrituras de propiedad podían incluir cauciones (cláusulas) según las cuales la propiedad objeto de la escritura no podía venderse a personas de una raza específica. El propósito de dichas cláusulas era nítido: hacer efectiva y perpetuar la segregación racial. Su uso estaba muy extendido, hasta el punto de que se estimaba que cuando la sentencia del caso «Shelley contra Kraemer»[60]

---

59 Véase *Madsen vs. Women's Health Center, Inc.*, 512 US 753, 785 (1994). Scalia se muestra de acuerdo con parte de la sentencia y disiente con respecto a otra parte: «El fallo de hoy [...] nos deja dolorosamente claro que ninguna regla o doctrina legal está a salvo de su anulación por parte de este Tribunal cuando se la aplica en un caso que afecte a la regulación estatal del aborto» [citando *Thornburgh vs. American College of Obstetricians and Gynecologists,* 476 US 747, 814, 1986 (escrito de desacuerdo de la jueza Sandra Day O'Connor)].

60 *Shelley vs. Kraemer,* 334 US 1, 1948.

derogó estas cláusulas por inconstitucionales, amparándose en el principio de protección igualitaria de todos los ciudadanos, el 25 % de las propiedades del sur de Chicago estaban escrituradas con la prohibición expresa de ser vendidas a afroamericanos.[61]

Por más abyectas que fueran estas cláusulas, hay que reconocerlas al menos cierta integridad. Y es que declaraban a las claras su propósito y dejaban ver los principios que afirmaban. Nadie podía fingir que la segregación que efectuaban constituía una suerte de subproducto achacable a decisiones tomadas en otro lugar. Aunque se trataba de cláusulas privadas, estaban respaldadas por el Estado y, de hecho, extraían de él todo su sentido. De este modo, las escrituras oficiales proclamaban públicamente: «Esta sociedad es racista».

Ahora bien, cuando el Tribunal Supremo derogó dichas cláusulas, la cuestión pasó a ser cómo se las podría reemplazar. Pocos esperaban que las actitudes subyacentes a estas cauciones legales desaparecieran repentinamente en virtud de un fallo judicial. De este modo, cuando el Tribunal erradicó la segregación directa, era de esperar la emergencia de una segregación indirecta que la sustituyera.

Y así fue, después de 1948, las comunidades locales modificaron sus técnicas para preservar la segregación racial, si bien en lugar de usar las cláusulas de las escrituras, recurrieron a la arquitectura. Las comunidades fueron diseñadas con el fin de «interrumpir el flujo» de residentes de unas a otras. En este sentido, se construyeron autopistas difíciles de atravesar o vías ferroviarias para desconectar físicamente unas comunidades de las otras. Las preferencias expresas de las cláusulas fueron reemplazadas por un millar de minúsculas trabas de arquitectura y zonificación. Formalmente nada prohibía la integración, pero los obstáculos informales se multiplicaron.[62]

---

61 Véase Herman H. Long y Charles S. Johnson, *People Versus Property: Race-Restrictive Covenants in Housing*, Nashville, Fisk University Press, 1947, pp. 32–33. Douglas S. Massey y Nancy A. Denton en *American Apartheid: Segregation and the Making of the Under Class*, Cambridge (Mass.) Harvard University Press, 1993, pp. 37-54, señalan que la *National Association of Real Estate Brokers* (Asociación Nacional de Agentes Inmobiliarios) incluyó en su código ético de 1924 un artículo que declaraba que «un agente inmobiliario nunca debe ser la vía de entrada en un barrio [...] de miembros de cualquier raza o nacionalidad [...] cuya presencia actuaría claramente en detrimento de los valores de la propiedad en ese barrio» (citando a Rose Helper, *Racial Policies and Practices of Real Estate Brokers*, Minneapolis, University of Minnesota Press, 1969, p. 201); los autores también indican que la *Fair Housing Authority* (Autoridad de Vivienda Pública) defendió el uso de cláusulas racistas hasta 1950 (citando a Kenneth T. Jackson, *Crabgrass Frontier: the Suburbanization of the United States*, Nueva York, Oxford University Press, 1985, p. 208).

62 Véase Massey y Denton, *American Apartheid, op. cit.*

Así pues, las administraciones locales optaron por una regulación muy similar a la que el gobierno federal impuso en el caso «Rust contra Sullivan» y a la que trató de imponer en el caso de «El Estado de Nueva York contra Estados Unidos»: inhabilitadas constitucionalmente para ejercer la segregación de forma directa, emplearon leyes de zonificación —arquitectura geográfica o código del espacio real— para llevarla a cabo indirectamente. De este modo, dichas administraciones locales diseñaron sus comunidades y sus calles con la intención de dificultar la integración, y estas trabas minúsculas de regulación por zonas demostraron una gran efectividad en ese sentido.

Lo que resulta más significativo de este caso, más aún que en el relativo al aborto, es que aquí se hace muy complicado percibir el vínculo entre la regulación y su efecto. La segregación que pervive entre las comunidades es descrita ahora como el producto de una «elección»: los individuos escogen vivir en un barrio en lugar de en otro. En un sentido estricto, esto sería cierto, pero hemos de enfatizar que sus elecciones han de afrontar los costes que el Estado ha impuesto sobre ellas. En consecuencia, como es más fácil mantenerse segregadas, las personas escogen esta opción, pero no hay que perder de vista que es más fácil porque el Estado ha removido Roma con Santiago para que así sea.

En este caso, el Estado está regulando de manera indirecta, empleando las estructuras del código del espacio real para alcanzar sus objetivos, si bien esta regulación, una vez más, no es percibida como tal. De esta forma, el Estado consigue producir el efecto deseado sin ningún coste político, beneficiándose de lo que claramente constituiría una regulación controvertida e ilegal sin ni siquiera tener que admitir que existe regulación alguna.

En los tres casos analizados, el Estado recurre al poder de otra modalidad de regulación —otra estructura de restricción— para llevar a cabo sus propios objetivos.[63] Esto no tiene por qué ser inadecuado por sí mismo, y, de hecho, existen

63 Michael Froomkin señala las regulaciones del chip *Clipper* como otro ejemplo de este procedimiento. Recurriendo al proceso de establecimiento de estándares para las compras estatales, el gobierno federal podría intentar conseguir un estándar de cifrado sin atenerse a la *Administrative Procedure Act* (Ley de Procedimiento Administrativo). «En el corazón de la estrategia del chip *Clipper* se encuentra un toque de genio burocrático. El Congreso nunca había concedido al Ejecutivo, y tampoco lo ha hecho hasta la fecha, el poder para controlar el uso privado de la criptografía. Ni siquiera le ha concedido el poder para establecer un sistema de depósito de claves secretas. Ante la ausencia de autoridades formales que eviten la adopción de criptografía que no se atenga a dicho depósito de claves, los defensores del *Clipper* dieron con la solución de usar el poder del Estado como consumidor a gran escala de productos criptográficos para manipular el mercado. De esta forma, por más que el Estado no pudiera impedir que la gente empleara productos no estandarizados, quizás podría imponer su estándar por medio de la compra e implementación masiva de productos con sistema de depósito de claves»; «It Came from Planet Clipper», *op. cit.*, pp. 15, 24, 31–33.

abundantes ejemplos al respecto que nadie calificaría de este modo. Así, por ejemplo, la exigencia de que las calles estén bien iluminadas supone una regulación diseñada para reducir los crímenes, y nadie la consideraría inadecuada. Tampoco la regulación de este tipo camufla su verdadera naturaleza. Pensemos de nuevo en los badenes —ejemplos de regulación indirecta— que, como en las carreteras sinuosas, utilizan el código de las calles para reducir la velocidad de los automóviles. En este caso, nadie se lleva a engaño acerca de la fuente de esta regulación; nadie cree que los badenes están ahí de forma accidental.

En resumidas cuentas, el argumento que vengo exponiendo no está en contra de la regulación indirecta en general, sino que se centra más bien en la transparencia. El Estado no tiene ningún derecho a camuflar sus propósitos. En una democracia constitucional, sus regulaciones deberían siempre ser públicas y, por lo tanto, uno de los asuntos que surgen al tratar la práctica de la regulación indirecta es la cuestión general de la publicidad. ¿Debería permitírsele al Estado el empleo de medios opacos de regulación cuando tiene a su disposición medios transparentes?

Adónde nos lleva esto

Después de publicar en la revista *The Industry Standard* (por entonces aún existía) un ensayo donde defendía que «el código es la ley»,[64] el editor recibió la siguiente misiva:

> Típico de un Profesor de Derecho de Harvard [...] Lessig pierde enteramente de vista el bosque mientras danza entre los árboles. [...] Por más que su agudo comentario sobre la oposición entre el Código de la Costa Oeste (el de los programadores de Silicon Valley) y el de la Costa Este (el de los juristas estatales) esté construido de forma muy inteligente, al final pasó completamente por alto la diferencia real entre ambos.
>
> El buen profesor parece aplicar el término «regulación» en el mismo sentido que los esfuerzos de las empresas privadas por *controlar la conducta de sus clientes mediante los mecanismos del mercado*, y que los esfuerzos de las agencias estatales por *controlar la conducta de todos los ciudadanos por medio de la fuerza de la ley*.

64 Véase *The Industry Standard*, disponible en http://www.lessig.org/content/standard/0,1902,4165,00.html.

> Mientras los creadores y proveedores del Código de la Costa Oeste (no importa cuán egoístas, monopolísticos, demoníacos o incompetentes puedan llegar a ser) no lleven pistolas o placas, no dudaré en elegirlos a ellos en lugar de a quienes aplican el Código de la Costa Este.[65]

Dejando de lado que haya pasado por alto o no la «diferencia real» entre el código y la ley, la genialidad de esta carta radica en que su autor percibe claramente la similitud real que existe entre ambos. El autor (presidente de un negocio relacionado con Internet) comprende que las «empresas privadas» intentan «controlar la conducta de sus clientes», y escribe que emplean «los mecanismos del mercado» para alcanzar tal control. (Una precisión técnica: yo hablaba del empleo de las arquitecturas para conseguir ese objetivo, pero no importa demasiado. Se haga a través del mercado o de la arquitectura, el argumento es el mismo). Por lo tanto, sí capta que existe «regulación» más allá de la ley, y simplemente señala cuál es su favorita (no en vano es ejecutivo de una corporación).

Lo que el autor de esta carta comprende es lo que todos nosotros debemos comprender para captar cómo está regulado el ciberespacio y cómo podría llegar a regularlo la ley. En este capítulo he sostenido que el Estado dispone de un repertorio de herramientas que utiliza para regular, y que dicho repertorio se expande en el ciberespacio. De forma indirecta, mediante la regulación de la escritura del código, el Estado puede alcanzar sus fines reguladores, a menudo sin padecer las consecuencias políticas que la persecución directa de esos mismos fines le acarrearía.

Esto debería suscitar nuestra preocupación. Deberíamos preocuparnos por un régimen que hace más fácil la regulación invisible, y también por un régimen que hace más fácil la regulación. Deberíamos preocuparnos por lo primero, porque la invisibilidad dificulta que nos resistamos a la mala regulación, y por lo segundo, porque —como sostengo en la Tercera Parte— todavía no hemos adquirido plena conciencia de los principios que están en riesgo ante el alcance creciente de una regulación eficaz.

Esto implica muchas preocupaciones, qué duda cabe. No obstante, antes de profundizar en ellas, podríamos examinar más detalladamente los contextos en los que estas preocupaciones se vuelven reales.

---

65 Véase «Legal Eagle» (carta al editor), *The Industry Standard*, 26 de abril de 1999 (la cursiva es mía).

8. Los límites del código abierto

Hasta ahora, he contado cómo funciona la regulación, y por qué deberíamos esperar un incremento de la regulabilidad de Internet. Tal y como describí, hablamos de cambios en la arquitectura de la Red que permitirán mejorar el control estatal, al facilitar la vigilancia de las conductas —o al menos su rastreo. Estos cambios surgirán incluso si el Estado no hace nada, como subproducto de los cambios destinados a favorecer el comercio electrónico. Ahora bien, la consolidación de tales cambios se producirá si (o cuando) el Estado entienda cómo esto podría poner la red a su servicio.

En esto ha consistido la Primera Parte. En ésta me he centrado en una regulabilidad diferente —el tipo de regulación que se efectúa a través de las arquitecturas del espacio donde uno vive. Como sostuve en el Capítulo 5, esta modalidad de regulación no es en absoluto novedosa: los Estados siempre han utilizado la arquitectura para regular la conducta. Lo que sí que resulta novedoso es la importancia que adquiere. A medida que la vida se traslade a la Red, una porción cada vez mayor de ella se regulará por medio del diseño deliberado del espacio donde dicha vida transcurre. Esto no es necesariamente algo malo. Así, si existiese una fórmula basada en el código que impidiera a gente conducir borracha, yo la apoyaría sin dudar. Ahora bien, esta regulación invasiva a través del código tampoco es benigna, porque, debido a su modo de funcionar, puede interferir con el proceso democrático ordinario mediante el cual exigimos responsabilidades a nuestros reguladores.

La crítica fundamental que he identificado hasta el momento apunta, pues, a la transparencia. La regulación mediante el código —especialmente cuando afecta a personas que no son técnicamente expertas— entraña el riesgo

de invisibilizar la propia regulación. Pese a que los controles impuestos responden a razones políticas concretas, la gente los experimenta como si fuesen naturales, lo cual, sugerí, podría debilitar la solidez de la democracia.

En estos momentos, una afirmación así tampoco dice mucho, al menos, a nosotros. Y es que nuestra cultura política está ya marcada en buena medida por la apatía, y nada sugiere que las cosas vayan a ser diferentes con respecto al ciberespacio. Es más, tal y como observa Castranova acerca de los mundos virtuales: «Qué extraño, pues, que apenas se encuentre democracia en los mundos sintéticos. De hecho, no hay ni rastro de ella. Ni el menor indicio de una sombra de un rastro de democracia. No existe. El modelo típico de gobierno en los mundos sintéticos consiste en momentos aislados de tiranía opresiva intercalados en medio de la anarquía generalizada».[1]

Si pudiéramos, no obstante, dejar de lado por un momento nuestro propio escepticismo acerca de nuestra democracia, y centrarnos en aspectos de Internet y del ciberespacio cuya importancia fundamental nadie discute, creo que todos podríamos reconocer un planteamiento que, una vez asumido, parece obvio: si el código regula, entonces, al menos en algunos contextos cruciales, la clase de código que regule revestirá una importancia igualmente crucial.

Al decir «clase» me refiero a la distinción entre dos tipos de código: abierto y cerrado. Entiendo «código abierto» como aquél (ya sea relacionado con software o con hardware) cuya funcionalidad resulta transparente al menos a alguien que conozca la tecnología en cuestión. Entiendo «código cerrado» como aquél (ya sea relacionado con software o con hardware) cuya funcionalidad es opaca. Es posible imaginar cómo funciona el código cerrado y, con suficiente tiempo para efectuar pruebas, se podría llegar a alterarlo mediante ingeniería inversa. Pero a partir de la tecnología en sí misma, no hay ningún modo razonable de discernir cuál es su funcionalidad.

Los términos «abierto» y «cerrado» aplicados al código evocarán para muchos un debate de vital importancia acerca de cómo debería desarrollarse el software. Lo que la mayoría llama el «movimiento de software de código abierto», pero que yo, siguiendo a Richard Stallman, denomino el «movimiento de software libre», defiende (al menos, en mi opinión) que existen valores fundamentales de libertad que exigen que el software que se desarrolle sea

1 Castranova, *Synthetic Worlds*, *op. cit.*, p. 207.

libre. En este sentido, lo contrario del software libre es el software propietario, aquél cuya funcionalidad oculta su desarrollador mediante la distribución de objetos digitales que mantienen la opacidad acerca del diseño subyacente.

Describiré este debate más a fondo a lo largo de este capítulo, pero es importante subrayar que mi argumentación respecto a la contraposición entre código «abierto» y código «cerrado» es distinta de la referida a cómo se crea el código. Personalmente, tengo ideas muy sólidas acerca de cómo debería crearse el código. Sin embargo, independientemente de la postura que tenga el lector en este debate, al menos en los contextos que voy a identificar aquí, deberíamos poder coincidir en dos puntos: primero, que el código abierto supone una restricción sobre el poder estatal, y, segundo, que al menos en ciertos casos, el código debe, de forma relevante, ser «abierto».

Con el fin de establecer el marco para este argumento, quiero describir dos contextos y defender que todos deberíamos coincidir en la importancia de la clase de código que se aplica en ellos. A partir de esto, el resto del capítulo se dedicará a exponer dicho argumento.

Bytes que fisgonean

En el Capítulo 2, describí una clase de tecnología que, cuando se publicó la primera edición de este libro, era un poco de ciencia ficción. En los cinco años siguientes, esa ficción ha devenido cada vez menos ficticia. En 1997, el Estado anunció un proyecto llamado *Carnivore*, destinado a construir una tecnología que hurgara en el tráfico de correos electrónicos y recopilara exclusivamente aquellos mensajes escritos por o a un individuo concreto e identificado. La intención del FBI era usar esta tecnología, contando con la correspondiente orden judicial, para reunir pruebas durante una investigación criminal.

En principio, hay muchas cosas elogiables en los ideales del diseño del *Carnivore*. Los protocolos exigían que un juez aprobara esta vigilancia y se pretendía que la tecnología sólo recopilara información acerca del objetivo de la investigación. De este modo, nadie más tendría que soportar el lastre de esta herramienta, nadie más tendría que ver comprometida su privacidad.

Ahora bien, para saber si la tecnología hacía lo que decía que iba a hacer había que remitirse a su código, y éste era cerrado.[2] El contrato que el Estado suscribió con el vendedor que desarrolló el *Carnivore* no requería que este software se hiciera público, sino que permitía que el vendedor mantuviera su código en secreto.

No es difícil entender por qué el vendedor deseaba mantener su código en secreto. Generalmente, invitar a otros a que observen el código que hemos escrito es muy parecido a invitarlos a cenar: hay mucho que preparar para que nuestra casa esté presentable. En este caso concreto, el Departamento de Justicia pudo haberse preocupado de la seguridad.[3] Sustantivamente, sin embargo, puede que el vendedor quisiera usar componentes del software en otros de sus proyectos. Si el código es público, la transparencia podría hacer que dicho vendedor perdiera cierta ventaja, lo que implica que al Estado le costaría más exigir una tecnología que revelara su código fuente. Así pues, la pregunta sería si el Estado gana algo exigiendo que se revele el código fuente.

Y he aquí el argumento obvio: como el Estado aprendió rápidamente al tratar de vender la idea del *Carnivore*, el hecho de que su código fuera secreto era costoso. Por más esfuerzos que consagró a intentar generar confianza en su proclama de que el *Carnivore* hacía sólo lo que decía que hacía, el argumento «soy del Estado, así que confía en mí» no tiene mucho peso. De esta forma, los esfuerzos estatales para desplegar esta tecnología —insisto, una tecnología valiosa si hacía lo que decía que hacía— tropezaron con múltiples obstáculos.

No conozco ningún estudio que haya intentado evaluar cuánto le costó al Estado este escepticismo acerca del *Carnivore* en comparación con lo que le habría costado desarrollarlo de forma abierta.[4] Me sorprendería que la estrategia del Estado tuviera sentido desde un punto de vista fiscal. No obstante, independientemente de que saliera más barato o más caro el desarrollo

---

2 Declan McCullagh, «It's Time for the Carnivore to Spin», *Wired News*, 7 de julio de 2000, disponible en http://www.wirednews.com/news/politics/0,1283,37590,00.html.

3 Ann Harrison, «Government Error Exposes Carnivore Investigators; ACLU Blasts Team for Close Ties to Administration», *Computerworld*, 5 de octubre de 2000, disponible en http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,51991,00.html. Esta preocupación fue duramente criticada. Véase *Center for Democracy and Technology*, «Cryptography», disponible en http://www.cdt.org/crypto/.

4 La corporación Mitre examinó para el ejército una cuestión relacionada con esto. Véase Carolyn A. Kenwood, *A Business Case Study of Open Source Software*, Mitre Corporation, 2001.

basado en código abierto, no debería ser objeto de controversia el hecho de que el Estado posee la obligación de hacer transparentes sus procedimientos —al menos en el contexto del encausamiento criminal ordinario. Con ello no quiero decir que el investigador tenga que revelar en qué piensa cuando decide centrarse en un sospechoso, sino que me refiero a los procedimientos que lleva a cabo para invadir los intereses de privacidad de los ciudadanos ordinarios.

La única clase de código que garantiza esa transparencia es el «código abierto», y la breve idea sobre la que deseo insistir por ahora es que allá donde importe la transparencia de la acción estatal, también debería hacerlo la clase de código que emplea el Estado. No estoy reclamando que todo el código estatal sea público. Creo que existen ámbitos legítimos en los que el Estado puede actuar en secreto; más específicamente, cuando la transparencia interfiere con la función misma. Sin embargo, hay una probabilidad muy limitada de que el posible sospechoso de un crimen pueda evadir con mayor efectividad la vigilancia del *Carnivore* sólo porque su código sea abierto. De ahí que me reafirme en mi convencimiento de que el código abierto debiera haber sido la norma aquí.

Máquinas que cuentan

Antes del 7 de noviembre de 2000, había muy poca discusión entre los políticos estadounidenses en torno a la tecnología de las máquinas de votación. Para la mayoría de la gente (entre la que me incluía), la cuestión de la tecnología de votación parecía algo trivial. Ciertamente puede que hubiera tecnologías de recuento de voto más rápidas, o tecnologías de comprobación de errores más precisas, pero la idea de que algo importante dependiera de estos detalles tecnológicos no era como para saltar a la portada del *New York Times*.

Las elecciones presidenciales de 2000 supusieron un vuelco en esta idea. Más concretamente, el vuelco vino provocado por el escrutinio en el Estado de Florida. Y es que la experiencia de Florida no sólo demostró la imperfección de los dispositivos mecánicos tradicionales de tabulación de votos (prueba número 1, la tarjeta electoral mal perforada), sino también la extraordinaria desigualdad que producía emplear diferentes tecnologías en diferentes partes del Estado. Como describió el juez Stevens en su voto

particular en el caso «Bush contra Gore», casi el 4 % de los votos mediante tarjeta perforada fue invalidado, mientras que sólo se invalidó el 1,43 % de los votos escrutados mediante lector óptico.[5] Además, según las estimaciones de un estudio, con sólo variar un voto en cada una de las máquinas, el resultado electoral habría cambiado.[6]

Las elecciones presidenciales de 2004 pusieron las cosas aún peor. En los cuatro años transcurridos desde la debacle de Florida, algunas compañías se habían puesto manos a la obra para implementar nuevas máquinas de votación electrónica. Sin embargo, estas máquinas generaron aún más ansiedad entre los votantes. Si bien la mayoría de ellos no son expertos en tecnología, todo el mundo experimenta la obvia inquietud que produce una máquina de votación completamente electrónica. La mecánica electoral sería la siguiente: nos situamos frente a un terminal y pulsamos los botones para indicar nuestro voto; la máquina nos solicita que lo confirmemos y, a continuación, nos informa de que el voto ha quedado registrado. Ahora bien, ¿cómo podemos estar seguros de ello? ¿Cómo podría alguien estar seguro? Incluso si no creemos tanto en la teoría de la conspiración como para pensar que todas las máquinas de votación están amañadas, ¿cómo puede alguien cerciorarse de que cuando estas máquinas vuelquen sus datos en el servidor central, éste registre su voto con precisión? ¿Qué garantía tenemos de que los resultados no serán manipulados?

El ejemplo más extremo de dicha ansiedad lo desencadenó Diebold, la compañía líder en votación electrónica. En 2003 se descubrió que esta empresa había manipulado las cifras asociadas a las pruebas de su tecnología de votación. La filtración de ciertos memorandos de Diebold reveló que la dirección de la compañía sabía que sus máquinas funcionaban defectuosamente y que, pese a ello, decidió intencionadamente ocultar este hecho. (La reacción de Diebold fue demandar a los estudiantes que habían filtrado los memorandos —por infracción de copyright—, pero éstos demandaron a su vez a la compañía en el mismo proceso judicial, y ganaron).

Este incidente pareció reforzar aún más a Diebold en sus actuaciones. Así, la compañía persistió en su negativa a revelar ningún dato acerca del código de sus máquinas, y rechazó participar en ningún concurso donde se

---

5 Véase *Bush vs. Gore*, 531 U.S. 98, 126, 2000 (Stevens, J., voto particular).

6 Di Franco *et al.*, «Small Vote Manipulations Can Swing Elections», *Communications of the ACM*, vol. 47, núm. 10, 2004, pp. 43–45, disponible en http://portal.acm.org/citation.cfm?id=1022621.

exigiera tal transparencia. Y si vinculamos este rechazo a la promesa del presidente de Diebold de «entregar Ohio» al presidente George W. Bush en el 2004, tendremos todos los ingredientes para que aparezcan nubarrones de desconfianza. Diebold controla las máquinas, Diebold no nos muestra cómo funcionan y Diebold promete un resultado específico en las elecciones. ¿Alguien duda de que la gente sospeche de la transparencia del proceso electoral?[7]

Y ahora resulta que nos percatamos de lo compleja que es la cuestión de cómo deberían diseñarse las máquinas de votación electrónica. En uno de mis momentos más mezquinos desde que cumplí veintiún años, le aseguré a un colega que no había razón alguna para celebrar un congreso sobre las votaciones electrónicas porque todas las cuestiones al respecto eran «perfectamente obvias». Y no sólo no eran perfectamente obvias, sino que, de hecho, eran muy complicadas de entender. A algunos les parecerá obvio que, como sucede con la tecnología de los cajeros automáticos, debería expedirse, como mínimo, un resguardo impreso. Ahora bien, si hay un resguardo impreso, se facilitaría que los votantes pudieran vender sus votos. Además, no hay razón para que el resguardo tenga que reflejar qué se computó ni tampoco qué se transmitió a cualquier autoridad central de tabulación. La cuestión de cómo definir el mejor diseño para estos sistemas resultó no ser tan obvia. Por lo que a mí respecta, después de haber pronunciado absolutas sandeces anteriormente, no entraré a considerar aquí cómo podría mejorarse esta arquitectura electoral.

Ahora bien, sea cual sea la arquitectura del sistema, hay una cuestión independiente en relación con la apertura del código que constituye dicho sistema. Una vez más, los procedimientos utilizados para tabular los votos deben ser transparentes. En el mundo no digital, esos procedimientos eran obvios; en el mundo digital, independientemente de su arquitectura, necesitamos un modo de asegurarnos que la máquina hace lo que se dice que hará. Una manera sencilla de asegurarnos es abrir el código de esas máquinas o, como mínimo, exigir que ese código venga certificado por inspectores independientes. Muchos preferirán esta última opción, y sólo porque la transparencia aquí podría aumentar las posibilidades de que el código fuera quebrantado por hackers. Mi intuición personal acerca de este asunto es diferente pero, sea o no completamente abierto el código, la exigencia de certificación resulta obvia. Y para que esta certificación funcione, el código de la tecnología debe ser —al menos en un sentido limitado— abierto.

---

7 Para un relato extraordinariamente inquietante que suscita mucho más que sospechas, véase Robert F. Kennedy, Jr., «Was the 2004 Election Stolen?», *Rolling Stone*, junio de 2006.

Estos dos ejemplos plantean un argumento similar que, sin embargo, no es universal; hay veces en que el código tiene que ser transparente, aunque que haya ocasiones en que no. No estoy hablando, pues, de todo el código aplicado a cualquier finalidad. No creo que Wal*Mart tenga que revelar el código que emplea para calcular el cambio en sus cajas de pago; ni siquiera que Yahoo! tenga que revelar el código de su servicio de mensajería instantánea. Pero sí creo que todos deberíamos coincidir en que, al menos en ciertos contextos, la transparencia del código abierto debería constituir una exigencia.

Éste es un argumento que Phil Zimmermann nos enseñó en la práctica hace más de quince años. Zimmermann escribió y lanzó a la red un programa llamado PGP (*pretty good privacy*, «privacidad bastante buena»). PGP proporciona privacidad y autentificación criptográficas, pero Zimmermann se dio cuenta de que no obtendría la confianza necesaria para ofrecer estos servicios en buenas condiciones a menos que abriera el código fuente de su programa. Así que, desde el principio (excepto por un breve lapso en que el programa fue propiedad de una compañía llamada NAI)[8] el código fuente estuvo disponible para que cualquiera pudiera revisarlo y verificarlo. Esta publicidad ha construido la confianza en el código —una confianza que nunca podría haberse producido mediante una mera orden. En este caso, el código abierto sirvió al propósito del programador, que consistía en construir confianza en un sistema que apoyaría la privacidad y la autentificación. Por lo tanto, el código abierto funcionó.

El difícil interrogante que se nos plantea ahora es si hay alguna exigencia que realizar más allá de esta mínima que se ha expuesto. He aquí la pregunta que nos ocupa en lo que queda de capítulo: ¿Cómo afecta el código abierto a la regulabilidad?

El código en la Red

A lo largo de este libro, he dedicado mucho tiempo a hablar sobre el «código». Ha llegado el momento de especificar un poco más qué es el «código» en el contexto de Internet, en qué sentido deberíamos considerar que dicho código es «abierto», y en qué contextos revestirá importancia su apertura.

---

8 David E. Ross, *PGP: Backdoors and Key Escrow*, 2003, disponible en http://www.rossde.com/PGP/pgp_backdoor.html.

Como he mencionado, la red de Internet está construida a partir de una combinación de protocolos a la que nos referimos conjuntamente con el nombre de TCP/IP. El conjunto TCP/IP incluye un gran número de protocolos que alimentan las diferentes «capas» de la Red. El modelo estándar para describir las capas de una red es el modelo de referencia OSI (*Open Systems Interconnect*, Interconexión de Sistemas Abiertos), que describe siete capas de red, cada una de las cuales representa una «función realizada cuando se transfieren datos entre aplicaciones que cooperan» a través de la Red. Ahora bien, el conjunto TCP/IP no está tan bien reflejado en ese modelo. Según Craig Hunt, «la mayoría de las descripciones del TCP/IP define entre tres y cinco niveles funcionales en la arquitectura del protocolo». En mi opinión, lo más sencillo es describir cuatro capas funcionales en una arquitectura TCP/IP,[9] que serían, en sentido ascendente, la capa de enlace de datos, la capa de red, la capa de transporte y la capa de la aplicación.[10]

Tres de estas capas constituyen la instalación esencial de fontanería de Internet, oculta tras las paredes de la Red. (Los grifos operan en la siguiente capa; sea paciente el lector). Al fondo del todo, justo por encima de la capa física de Internet, en la capa de enlace de datos, operan muy pocos protocolos, ya que ésta maneja exclusivamente las interacciones de red local. En la capa inmediatamente superior, la de red, existen más protocolos, siendo dominante el protocolo IP, que envía los datos entre anfitriones y a través de enlaces de red, determinando qué ruta deberán tomar dichos datos. En la siguiente capa, la de transporte, dominan dos protocolos diferentes —el TCP y el UDP—, encargados de negociar el flujo de datos entre dos anfitriones de red. (La diferencia entre ellos se basa en su fiabilidad —el UDP no ofrece garantías).

Estos protocolos funcionan conjuntamente como una especie de empresa de mensajería muy peculiar. Los datos pasan de la capa de aplicación a la de transporte, donde los datos se empaquetan en una caja (virtual) sobre

---

9 Craig Hunt, *TCP/IP: Network Administration*, Sebastopol (Calif.), O'Reilly and Associates, 1997, pp. 1–22; Loshin, *TCP/IP: Clearly Explained*, *op. cit.*, pp. 13–17.

10 No existe un modelo de referencia estándar para las capas del TCP/IP. Hunt se refiere a ellas como las capas de «acceso a la red», de «internet», de «transporte de anfitrión a anfitrión» y de «aplicación» en *TCP/IP: Network Administration*, *op. cit.*, p. 9. Loshin usa la terminología que yo sigo en el texto en *TCP/IP: Clearly Explained*, *op. cit.*, pp. 13–17. Pese a la diferencia nominal, las funciones realizadas en cada una de estas capas son coherentes. Al igual que con cualquier modelo de pila, los datos «descienden por la pila de protocolos cuando se envían a la red, y escalan la pila cuando se reciben desde la red». Cada capa «posee sus propias estructuras de datos independientes» e «ignora las estructuras de datos usadas por» las otras capas; Hunt, *TCP/IP: Network Administration*, *op. cit.*, p. 9.

la que se pega una etiqueta (virtual). Esta etiqueta asocia los contenidos de la caja a unos procesos particulares. (Ésta es la tarea de los protocolos TCP y UDP). Hecho esto, la caja pasa a la capa de red, donde el protocolo IP la coloca dentro de otro paquete que lleva su propia etiqueta, la cual incluye las direcciones de origen y de destino. A partir de aquí, ese paquete puede envolverse de nuevo en la capa de enlace de datos, dependiendo de las especificaciones de la red local (si, por ejemplo, es una red Ethernet).

Por lo tanto, todo este proceso supone un intrincado juego de embalaje: en cada capa se añade una nueva caja, y la nueva etiqueta que se pega en cada caja describe el proceso que ocurre en esa capa. Al otro extremo, el proceso de embalaje se invierte: como una muñeca rusa, cada envoltorio se abre en la capa correspondiente, hasta que al final la máquina recupera los datos de aplicación iniciales.

Por encima de estas tres capas se encuentra la capa de aplicación de Internet, donde los protocolos «proliferan».[11] Entre ellos se encuentran los protocolos de aplicación de red que nos resultan más familiares, como el FTP (*File Transfer Protocol*, para la transferencia de archivos), el SMTP (*Simple Mail Transport Protocol*, para la transferencia de correo) y el HTTP (*Hyper Text Transfer Protocol*, un protocolo para publicar y leer documentos hipertexto a través de la Red). Se trata de reglas que definen cómo un cliente (nuestro ordenador) interactuará con un servidor (donde se albergan los datos), o con otro ordenador (en las redes P2P), y viceversa.[12]

Estas cuatro capas de protocolos conforman «Internet». Construido sobre bloques simples, el sistema posibilita una extraordinaria variedad de interacción. Quizá no sea tan fascinante como la naturaleza —piense el lector en el ADN—, pero se construye siguiendo el mismo principio: si se mantiene la simplicidad de los elementos, las combinaciones resultarán extraordinarias.

---

11 Hunt, *TCP/IP: Network Administration*, *op. cit.*, p. 9; Loshin, *TCP/IP: Clearly Explained*, *op. cit.*, pp. 13–17.

12 Tal y como explican Hafner y Lyon: «La opinión general decía que cualquier protocolo era un potencial módulo, de modo que el mejor enfoque pasaba por definir protocolos simples y limitados en sus respectivos alcances, con la expectativa de que cualquiera de ellos podría ensamblarse o modificarse de varias maneras imprevistas. La filosofía de diseño de protocolos adoptada por el NWG [*network working group*, grupo de trabajo de la red de ARPANET] puso la primera piedra de lo que llegaría a aceptarse ampliamente como el enfoque "por capas" de los protocolos»; *Where Wizards Stay Up Late*, *op. cit.*, p. 147.

Cuando hablo de regular el código, no me refiero a modificar este conjunto de protocolos fundamentales (aunque, en principio, podría ser regulado, y ya ha sido propuesto).[13] Desde mi perspectiva, estos componentes de la red son fijos, de modo que si exigiésemos que fueran diferentes, descompondríamos Internet. Por consiguiente, más que imaginar al Estado modificando el núcleo de la red, la cuestión que deseo considerar aquí es cómo el Estado podría (1) complementar dicho núcleo con tecnología que acreciente la regulabilidad, o bien (2) regular las aplicaciones que se conectan al núcleo. Ambas opciones son importantes, pero me gustaría centrar la atención en el código que se conecta a Internet, al que denominaré el «espacio de aplicación» de Internet. Este espacio incluye todo el código que implementa el conjunto de protocolos TCP/IP en la capa de aplicación —navegadores, sistemas operativos, módulos de cifrado, Java, sistemas de correo electrónico, aplicaciones P2P y cualesquiera otros elementos. El interrogante que abordaremos en el resto del capítulo es: ¿cuál es la característica de ese código que lo hace susceptible de regulación?

---

13 Las batallas en torno al cifrado en el nivel de enlaces, por ejemplo, son batallas en torno al conjunto de protocolos TCP/IP. Algunos representantes de la industria de redes han propuesto que el cifrado se lleve a cabo en las puertas de enlace, con un método para volcar texto sin formato en las propias puertas de enlace si existiera la correspondiente autorización legal —una especie de «timbre privado» para resolver la controversia en torno al cifrado; véase Elizabeth Kaufman y Roszel Thomsen II, «The Export of Certain Networking Encryption Products Under ELAs», disponible en http://www.cisco.com/web/about/gov/downloads/779/govtaffs/ archive/CiscoClearZone.doc. A este método se ha opuesto el IAB (*Internet Architectural Board*, Consejo de Arquitectura de Internet) por considerarlo incoherente con la arquitectura «punto a punto» de Internet; véase la declaración del IAB sobre el cifrado de «timbre privado», disponible en http://www.iab.org/documents/docs/121898.html.

Desde la aparición de la primera versión de *El Código*, se ha producido una explosión de obras excelentes que se extienden sobre la «teoría de capas». Acaso la mejor obra académica en este campo haya sido Lawrence B. Solum y Minn Chung, «The Layers Principle: Internet Architecture and the Law», *Public Law and Legal Theory*, Universidad de San Diego, informe de investigación núm. 55, disponible en http://ssrn.com/abstract=416263. Solum y Chung han empleado la idea de las capas de Internet para guiar las políticas de regulación, localizando objetivos adecuados e inadecuados de la intervención reguladora. Éste es un ejemplo del mejor trabajo de integración entre tecnología y políticas legales, extrayendo implicaciones interesantes e importantes de la interacción específica, a veces contraria a la intuición, que se da entre ellas. Yo introduje las «capas» en mi propio trabajo en *The Future of Ideas: The Fate of the Commons in a Connected World*, Nueva York, Random House, 2001, pp. 23–25. Véase también Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven, Yale University Press, 2006, pp. 391–397. Para otras obras muy útiles que extienden este análisis, véase Craig McTaggart, «A Layered Approach to Internet Legal Analysis», *McGill Law Journal*, núm. 48, 2003, p. 571; Thomas A. Lane, «Of Hammers and Saws: The Toolbox of Federalism and Sources of Law for the Web», *New Mexico Law Review*, núm. 33, 2003, p. 115; Jane Bailey, «Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation», *Manitoba Law Journal*, núm. 30, 2004, p. 197.

Una breve historia del código en la Red

Al principio, por supuesto, había muy pocas aplicaciones en la Red. Ésta no era más que un protocolo para el intercambio de datos, y los programas originales simplemente aprovechaban este protocolo. El protocolo de transferencia de archivos (FTP) nació en los comienzos de su historia de la Red;[14] el protocolo de transferencia de mensajes electrónicos (SMTP) lo hizo poco después. Y no hubo que esperar mucho para que se desarrollara un protocolo para mostrar directorios de un modo gráfico (Gopher). Y en 1991 el protocolo más famoso —el protocolo de transferencia de hipertexto (HTTP) y el lenguaje de etiquetas de hipertexto (HTML) —propició el nacimiento de la *World Wide Web*.

Cada protocolo engendró muchas aplicaciones. Dado que nadie ostentaba un monopolio sobre el protocolo, nadie lo ostentaba tampoco sobre su implementación. Así, había muchas aplicaciones FTP y muchos servidores de correo electrónico; incluso había un elevado número de navegadores.[15] Los protocolos eran estándares abiertos que recibían la bendición de los organismos de estandarización como el IETF y, posteriormente, el W3C. Una vez que se especificaba un protocolo, los desarrolladores podían construir programas que lo utilizaran.

Buena parte del software que implementaba estos protocolos era «abierto», al menos inicialmente —esto es, el código fuente del software estaba disponible junto con el código objeto.[16] Esta apertura fue la responsable de gran parte del crecimiento inicial de la Red, puesto que otros podían explorar cómo se implementaba un programa y aprender de ese ejemplo para implementar mejor el protocolo en el futuro.

---

14 Véase Hafner y Lyon, *Where Wizards Stay up Late*, *op. cit.*, p. 174.

15 Un manual de HTML de 1994 enumera veintinueve navegadores diferentes; véase Larry Aronson, *HTML Manual of Style*, Emeryville (Cal.), Ziff-Davis Press, 1994, pp. 124–126.

16 El código fuente es el código que escriben los programadores. A veces se lee de forma parecida al lenguaje natural, pero obviamente no coincide con él. Un programa se escribe (usualmente) en código fuente, pero para ser ejecutado debe convertirse a un lenguaje que pueda procesar el ordenador, lo cual se hace mediante un «compilador». Algunos códigos fuente se convierten sobre la marcha —el lenguaje de programación BASIC, por ejemplo, es normalmente interpretado, lo que implica que el ordenador compila el código fuente a medida que se ejecuta. El «código objeto» es legible por máquinas y se compone de una cadena de «ceros» y «unos» que da instrucciones a la máquina acerca de las tareas que ha de realizar.

La *World Wide Web* representa el mejor ejemplo de ello. Insisto, el código que permite que una página web aparezca tal y como lo hace es el lenguaje de marcado de hipertexto, o HTML,[17] con el que podemos especificar cómo se mostrará una página web y a qué estará vinculada.

El HTML original fue propuesto en 1990 por los investigadores del CERN (*Conseil Européen pour la Recherche Nucléaire*, Consejo Europeo para la Investigación Nuclear) Tim Berners-Lee y Robert Cailliau.[18] Este lenguaje se diseñó para facilitar la vinculación de documentos en el marco de los centros de investigación, pero rápidamente se hizo obvio que con él podrían enlazarse los documentos de cualquier máquina conectada a Internet. Berners-Lee y Cailliau decidieron abrir tanto el HTML como su compañero, el HTTP, para que cualquiera dispusiera de ellos libremente.

Y eso es precisamente lo que hizo la gente, al principio con lentitud, pero luego con una aceptación extraordinaria. La gente empezó a construir páginas web y a vincularlas con otras, hasta el punto que el HTML se convirtió en uno de los lenguajes de computación que más velozmente ha crecido en la historia de la informática.

¿Por qué? Una razón fundamental es que el HTML siempre fue «abierto». Incluso hoy, en la mayoría de los navegadores que se distribuyen, siempre tenemos la opción de revelar la «fuente» de una página web para ver cómo está «marcada». La fuente permanece abierta: podemos descargarla, copiarla y mejorarla como deseemos. Las leyes de copyright pueden proteger el código fuente de una página web, pero en realidad lo hacen de un modo muy imperfecto. Si el HTML llegó a ser tan popular fue primordialmente porque resultaba muy fácil de copiar. Cualquiera, en cualquier momento, podía mirar «debajo del capó» de un documento HTML y aprender cómo lo produjo su autor.

La apertura —no la propiedad o el contrato, sino el código y el acceso libres— creó la explosión que propiciaría el nacimiento de la Internet que todos conocemos. Y esto, a su vez, atrajo la atención del comercio, que razonó acertadamente «seguro que de toda esta actividad se puede obtener dinero».

---

17 El hipertexto es un texto vinculado a otra parte del mismo documento o a otro documento situado en la Red o en el mismo ordenador.

18 T. Berners-Lee y R. Cailliau, *WorldWideWeb: Proposal for a HyperText Project*, 1990, disponible en http://www.w3.org/Proposal.

Históricamente el modelo comercial de producción de software ha sido diferente.[19] A pesar de que la historia comenzó cuando el movimiento de código abierto aún continuaba en marcha, los vendedores de software comercial no estaban por la labor de producir software «libre» (lo que la mayoría denomina software «de código abierto»). Así pues, estos vendedores produjeron software cerrado —es decir, software que viajaba sin su código fuente y que estaba protegido contra la modificación tanto por la ley como por su propio código.

Hacia la segunda mitad de la década de los noventa —marcada especialmente por el lanzamiento por parte de Microsoft del sistema operativo Windows 95, que venía instalado especialmente para Internet— los vendedores de software comercial comenzaron a producir código del «espacio de aplicación». Este código cada vez estaba más conectado a la Red —cada vez se convertía más en código «en» Internet—, pero, en su mayor parte, permanecía cerrado.

Sin embargo, esto empezó a cambiar en los albores del siglo XXI. Especialmente en el contexto de los servicios P2P, surgieron tecnologías que eran dominantes y «abiertas». Más importante aún, los protocolos de los que dependían estas tecnologías no estaban regulados. Así, por ejemplo, el protocolo que el cliente P2P Grokster usaba para compartir contenido a través de Internet es un estándar abierto que cualquiera puede emplear. Muchas entidades comerciales intentaron usar ese estándar, al menos hasta la sentencia de 27 de junio de 2005 por la que el Tribunal Supremo falló contra dicho cliente en el «caso Grokster».[20] Ahora bien, por más que esta decisión judicial llevó a todas las entidades comerciales a abandonar la red StreamCast, siguieron existiendo implementaciones no comerciales del protocolo.

La misma combinación entre código abierto y código cerrado se da tanto en los navegadores como en el software de los blogs. Firefox es la implementación actualmente más en boga de la tecnología Mozilla —la tecnología en la que se basó originalmente el navegador Netscape—, compitiendo con Internet Explorer de Microsoft y con un puñado de otros navegadores comerciales. De igual forma, WordPress es una herramienta abierta de creación de blogs que compite con otras herramientas propietarias con la misma función.

---

19 Por supuesto, no siempre ha sido así. Cuando comenzó la producción comercial de ordenadores, el software solía ser un añadido gratuito al ordenador. Su desarrollo comercial como software propietario vendría después; véase Ira V. Heffan, «Copyleft: Licensing Collaborative Works in the Digital Age», *Stanford Law Review*, núm. 49, 1997, pp. 1487, 1492–1493.

20 Véase *MGM Studios, Inc. vs. Grokster, Ltd.*, 545 U.S. 913, 2005. [N. del E.]

Este crecimiento reciente del código abierto se basa en una larga tradición, parte de cuya motivación es ideológica, o basada en principios. En este sentido, Richard Stallman representa la fuente de inspiración principal. En 1984 Stallman creó la FSF (*Free Software Foundation*, Fundación para el Software Libre) con el propósito de impulsar el crecimiento del software libre. Premiado en 1990 con la prestigiosa beca MacArthur, este programador estadounidense abandonó a mediados de la década de los setenta su carrera académica para consagrar su vida al movimiento de software libre. De este modo, comenzó su trabajo con el lanzamiento del proyecto GNU, que pretendía desarrollar un sistema operativo libre. En 1991 el proyecto GNU contaba ya prácticamente con todo lo que necesitaba, excepto un núcleo (*kernel*, en alemán). Este último reto fue asumido por un estudiante de la Universidad de Helsinki llamado Linus Torvalds. Ese año, Torvalds publicó en Internet el núcleo de un sistema operativo e invitó a todo el mundo a extenderlo y a experimentar con él.

El mundo respondió a su invitación y, poco a poco, a principios de los años noventa, la gente fue combinando el proyecto GNU con el núcleo de Torvalds hasta construir un sistema operativo completo —GNU/Linux. Hacia 1998, todos habían comprendido ya que GNU/Linux iba a convertirse en un importante competidor para el sistema operativo de Microsoft. Puede que Microsoft imaginara en 1995 que para el año 2000 no existiría más sistema operativo de servidores que su Windows NT, pero cuando llegó el año 2000, ahí estaba GNU/Linux, representando una seria amenaza para Microsoft en el mercado de los servidores. Actualmente, en 2007, los servidores web basados en GNU/Linux siguen ampliando su mercado a costa de los sistemas de Microsoft.

El sistema operativo GNU/Linux es asombroso en múltiples aspectos. En primer lugar porque es teóricamente imperfecto pero superior a efectos prácticos. Linus Torvalds rechazó lo que la ciencia informática de la época dictaba como el diseño ideal de sistemas operativos,[21] y en lugar de ello construyó un sistema operativo diseñado para un solo procesador (un Intel 386)

21 En la época en que se desarrolló Linux, el pensamiento dominante entre los científicos informáticos estaba en contra del diseño de un sistema operativo monolítico que se basara en un único núcleo y a favor del diseño de un sistema basado en «micronúcleos» (*microkernel*). MINIX, un sistema desarrollado ortodoxamente, fue el primer competidor de Linux en ese momento. Torvalds rechazó conscientemente este pensamiento «moderno» y adoptó para Linux el modelo «tradicional»; véase «The Tanenbaum-Torvalds Debate», en Chris DiBona *et al*. (eds.), *Open Sources: Voices from the Open Source Revolution*, Sebastopol (Cal.), O'Reilly and Associates, 1999, pp. 221–251.

e incompatible con otras plataformas. Su desarrollo creativo y la energía que éste inspiró convirtieron poco a poco GNU/Linux en un sistema extraordinariamente potente. En el momento de escribir estas líneas, GNU/Linux ha sido adaptado, como mínimo, a dieciocho plataformas diferentes de arquitectura informática —de los procesadores Intel originales a dispositivos móviles que usan procesadores ARM.[22] Algunos hackers creativos incluso han adaptado Linux al iPod de Apple o a los antiguos sistemas Atari. Así, aunque inicialmente se concibiera para hablar sólo un lenguaje, GNU/Linux se ha convertido en la *lingua franca* de los sistemas operativos libres.

Lo que determina que un sistema operativo sea abierto es el compromiso de sus desarrolladores de mantener siempre público su código fuente —esto es, mantener siempre abierto el capó del coche. Tal compromiso no se queda sólo en un deseo; Stallman lo codificó jurídicamente en una licencia que establece los términos que controlan el uso futuro de la mayoría del software libre. Se trata de la GPL (*General Public License*, Licencia Pública General) lanzada por la FSF, una licencia que exige que cualquier código que se acoja a ella (como lo hace GNU/Linux) mantenga público su código fuente. GNU/Linux fue desarrollado por una extraordinaria conjunción de hackers de todo el mundo simplemente porque su código estaba abierto para que otros siguieran trabajando sobre él.

En otras palabras, su código se asienta sobre el *procomún*:[23] cualquiera puede tomarlo y usarlo como desee; cualquiera puede tomarlo y llegar a comprender cómo funciona.[24] El código de GNU/Linux es como un programa de

---

22 Véanse las listas «Ports of Linux» y Linux Online, «Hardware Port Projects», disponibles en http://www.cyut.edu.tw/~ckhung/l/linux_ports.html y en http://www.linux.org/projects/ports.html.

23 Técnicamente, el código libre no se asienta sobre el dominio público. El código de estos proyectos abiertos se ampara en las leyes de copyright y se publica bajo una licencia. Así, GNU/Linux se publica bajo la licencia GNU GPL, que limita el posible uso que se puede hacer del sistema operativo; esencialmente, no se puede tomar la parte pública y cerrarla, y tampoco se la puede integrar con código cerrado; véase Bruce Perens, «The Open Source Definition», en DiBona *et al*. (eds.), *Open Sources*, *op. cit.*, pp. 181–182. De esta forma, a efectos de futuros desarrollos de código abierto, el código se asienta sobre el procomún. Acerca de la idea y de los principios de los *commons*, véase, por ejemplo, Michael A. Heller, «The Tragedy of the Anticommons: Property in the Transition from Marx to Markets», *Harvard Law Review*, núm. 111, 1998, p. 621; Stephen M.McJohn, «Fair Use and Privatization in Copyright», *San Diego Law Review*, núm. 35, 1998, p. 61; Mark A. Lemley, «The Economics of Improvement in Intellectual Property Law», *Texas Law Review*, núm. 75, 1997, p. 989; Mark A. Lemley, «Romantic Authorship and the Rhetoric of Property», *Texas Law Review*, núm. 75, 1997, p. 873; Jessica Litman, «The Public Domain», *Emory Law Journal*, núm. 39, 1990, p. 965; Carol M. Rose, «The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems», *Minnesota Law Review*, núm. 83, 1998, p. 129.

24 En los últimos años, tanto en el seno del movimiento de software libre como en el más

investigación cuyos resultados son continuamente publicados para que los demás puedan verlos. Todo en él es público; cualquiera puede sumarse al proyecto sin tener que pedir permiso a nadie.

Este proyecto ha sido mucho más exitoso de lo que nadie imaginó nunca: en 1992 la mayoría de la gente habría afirmado que era imposible construir un sistema operativo libre a partir del trabajo de voluntarios repartidos por todo el mundo; en 2002 nadie podía ponerlo en duda. Ahora bien, si lo imposible pudo hacerse posible, entonces sin duda podría volverse imposible de nuevo. Y ciertas tendencias en la tecnología informática pueden generar precisamente esa amenaza.

Por ejemplo, consideremos el modo en que el código de ASP (*Active Server Pages*, Páginas Activas de Servidor) funciona en la Red. Cuando se accede a una página ASP en Internet, el servidor ejecuta un programa —una secuencia de comandos que da acceso a una base de datos, por ejemplo, o a un programa para generar los nuevos datos que se necesiten. Estas páginas

---

amplio (y heredero reconocido del anterior) movimiento por la cultura libre, ha venido ganando aceptación la traducción castellana del término inglés *commons* (literalmente, terrenos o bienes comunales) por «procomún». Más allá de la escueta acepción como «utilidad pública» que recoge el Diccionario de la Real Academia Española, Miquel Vidal definió así este concepto en el documento de presentación de las II Jornadas Copyleft de Barcelona celebradas en 2004 (disponible en http://www2.unia.es/arteypensamiento04/ezine/ezine04/abr00.html):

> El viejo vocablo castellano «procomún» –que alude a los espacios y recursos colectivos cuyo aprovechamiento y gestión se realiza de forma comunal– puede servirnos de forma más precisa y general que la expresión inglesa *copyleft* para encontrar un punto de conexión entre las distintas prácticas (musicales, literarias, de software libre...) que han surgido en los últimos años frente al copyright restrictivo. Desde una perspectiva jurídica, todos los ciudadanos tienen acceso libre a los bienes y recursos englobados bajo el procomún, aunque deben respetar ciertas reglas (que varían en cada caso). Es un derecho civil que no se ciñe exclusivamente al ámbito mercantil, sino que se inserta en una dinámica social mucho más amplia y compleja. De este modo, fomenta no sólo el beneficio económico de los autores (como hace el copyright), sino también el enriquecimiento creativo y comunitario de todos los agentes implicados en los procesos de transferencia de información y conocimiento.

En el artículo «Los cuatro entornos del procomún» (publicado en el monográfico que la revista *Archipiélago* dedicó al procomún en su número 77-78 de noviembre de 2007), Antonio Lafuente, investigador del Instituto de Historia del CSIC, retoma estas reflexiones y precisa la definición de procomún de esta forma:

> Lo que aquí nos interesa es subrayar cómo hemos ido apartándonos de la noción de propiedad para adentrarnos en la de comunidad. Y es que es imposible evitar lo que es obvio: el procomún, los bienes comunes –los *commons*, en inglés– sostienen y son sostenidos por colectivos humanos. Y, así, salimos de la economía y nos metemos en la antropología. [...] De la ética de los valores hemos de transitar a la de las capacidades si queremos entender cómo es la dinámica de producción del procomún, pues un bien común no es más que una estrategia exitosa de construcción de capacidades para un colectivo humano [p. 16].

[N. del E.]

ASP representan una forma cada vez más popular de proporcionar mayor funcionalidad al programa. Mientras se navega a través de Internet, esta tecnología está siempre en uso.

Sin embargo, el código que ejecuta las ASP no está técnicamente «distribuido», por lo que, incluso si se hubiera producido a partir de código bajo licencia GPL, no le sería aplicable la obligación de liberarlo para los demás que está recogida en la GPL. En consecuencia, a medida que cada vez más infraestructuras de la vida en la Red pasen a estar gobernadas por la tecnología ASP, cada vez se liberarán menos parcelas bajo licencias libres.

La «informática de confianza» crea otra amenaza para la ecología del código abierto. Lanzada como una respuesta a los virus y a las amenazas a la seguridad en un entorno de red, el atributo técnico clave de esta «informática de confianza» consiste en que la plataforma bloquea aquellos programas que no estén firmados mediante criptografía o verificados por la plataforma. Por ejemplo, si deseamos ejecutar un programa en nuestro ordenador, éste verificará antes que dicho programa viene certificado por una de las autoridades reconocidas por el sistema operativo, y que «incorpora los estándares de seguridad de hardware y software [...] aprobados por los propios proveedores de contenido».[25] Si no es así, el programa no se ejecutará.

En principio, por supuesto, si el coste de obtener el certificado de un programa fuera minúsculo, esta limitación no supondría ningún problema. El temor radica, sin embargo, en que esta restricción opere para bloquear en la práctica los proyectos de código abierto. No es fácil para una autoridad de certificación llegar a conocer qué hace un programa, lo cual implica que no estarán muy dispuestas a certificar programas en los que no puedan confiar. Esto, a su vez, supondrá una discriminación significativa contra el código abierto.

Regulando el código abierto

Los proyectos de código abierto —ya sean proyectos de software libre o de software de código abierto— comparten la característica de que todos pretenden que el conocimiento necesario para copiar el proyecto esté a disposición

---

25 Daniel Benoliel, «Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology», *California Law Review*, núm. 92, 2004, pp. 1069, 1114.

de los demás. El desarrollador de un proyecto de código abierto no efectúa ni un solo esfuerzo, sea éste legal o tecnológico, para que dicho desarrollo sea exclusivo. Y, más importante aún, también se preserva la capacidad de copiar y cambiar de la forma más eficaz la dirección de un proyecto dado.

¿Cómo afecta este hecho a la regulabilidad del código?

En el Capítulo 5 esbocé una serie de ejemplos en los que el Estado regulaba el código. Retomemos ahora dichos ejemplos: ¿cómo funciona tal regulación?

Consideremos dos de esos ejemplos. En el primero, el Estado señala a las compañías telefónicas algo acerca de cómo han de diseñar sus redes; en el segundo, el Estado señala a los fabricantes de televisores los tipos de chips que han de implantar en sus aparatos. ¿Cómo funcionan estas regulaciones?

En ambos casos, la respuesta es obvia. El código es regulable únicamente porque los desarrolladores de código pueden ser controlados. Si el Estado le ordena a una compañía telefónica que haga algo, es poco probable que ésta se resista, ya que le acarrearía una sanción; las sanciones son caras y las compañías telefónicas, como cualquier otra compañía, desean reducir los costes de hacer negocios. Si la regulación estatal es racional (esto es, efectiva), establecerá el coste de desobedecerla por encima de cualquier otro posible beneficio. Si el objetivo de la regulación es un actor racional que está al alcance del Estado, entonces es probable que la regulación produzca el efecto deseado. La regulación que la mencionada CALEA establecía con respecto a la arquitectura de red de los teléfonos representa un ejemplo obvio (véase el Capítulo 5).

Así pues, un destinatario de la regulación que sea inamovible e inmóvil supone un buen comienzo para la regulabilidad. Esta afirmación posee un interesante corolario: el código regulable es el código cerrado. Reflexionemos de nuevo acerca de las redes telefónicas. Cuando el Estado induce a las compañías telefónicas a modificar el software de sus redes, los usuarios no pueden elegir de ninguna forma si adoptan o no esta modificación. Cuando descolgamos el teléfono, escuchamos el tono de marcado que nos proporciona la compañía, y no conozco a ningún hacker que haya modificado el código de la compañía telefónica para construir un diseño de red diferente. Lo mismo ocurre con el chip V —dudo que exista mucha gente que se arriesgara a destruir su televisor para extraerle el chip, y estoy seguro de que nadie reimplantaría después el chip para introducir una tecnología diferente de filtros.

En ambos casos, la regulación del Estado funciona porque, una vez que el destinatario de la regulación cumple con ella, a los clientes apenas les queda más opción que aceptarla.

El código abierto es diferente, y podremos captar algo de esta diferencia en una historia contada por el ex asesor legal de Netscape, Peter Harter, un relato acerca del propio Netscape y los franceses.[26]

En 1996 Netscape hizo público un protocolo (SSL v3.0) para facilitar el comercio electrónico seguro en Internet. La esencia de su función era permitir el intercambio seguro entre un navegador y un servidor, lo cual no les hizo demasiada gracia a los franceses. Éstos expresaron su deseo de poder interceptar las transacciones realizadas mediante este protocolo, solicitando a Netscape que modificase el SSL para permitirles espiar dichas transacciones.

Existen muchas restricciones en la capacidad de Netscape para modificar el protocolo —la menor de las cuales no era el hecho de que Netscape había puesto a disposición pública el SSL, bajo la forma de un estándar público. No obstante, asumamos por un momento que no lo hubiera hecho así, y que Netscape realmente controlase los estándares del SSL y pudiera teóricamente modificarlo para permitir el espionaje francés. ¿Significaría eso que Netscape podría llevar a efecto la solicitud francesa?

No. Técnicamente, podría hacerlo mediante la modificación del código del Netscape Communicator y la posterior publicación de un nuevo modelo que permitiera la intrusión estatal. Ahora bien, como el código de Netscape (o, más generalmente, del proyecto Mozilla) es abierto, cualquiera es libre de construir un módulo alternativo que sustituya al módulo *afrancesado* del SSL. Tal módulo competiría con otros diferentes y ganaría aquél que eligieran los usuarios. Y a éstos no les suele agradar un módulo que permita el espionaje estatal.

El argumento es simple, pero sus implicaciones son profundas. En la medida en que el código sea abierto, el poder estatal se ve restringido. Por mucho que el Estado exija y amenace, cuando el destinatario de su regulación tiene un carácter plástico, no puede confiar en que cumpla sus dictados.

---

26 Peter Harter, «The Legal and Policy Framework for Global Electronic Commerce», comentarios en el Congreso del *Berkeley Center for Law and Technology*, 5-6 de marzo de 1999.

Imagínese el lector que es un propagandista soviético ansioso de que la gente lea un montón de información acerca de «Papá» Stalin. Para ello, el lector declara que todo libro que se publique en la Unión Soviética ha de incluir un capítulo dedicado a Stalin. ¿Qué probabilidad hay de que esos capítulos afecten realmente a lo que la gente lee?

Los libros son *en sí* código abierto: no ocultan nada, sino que revelan su código fuente —¡ellos mismos son su código fuente! El usuario de un libro (el que adopta la tecnología libresca) siempre tiene la opción de leer exclusivamente aquellos capítulos que más le gusten. Si se trata de un libro sobre electrónica, ciertamente puede que el lector decida saltarse el capítulo sobre Stalin, y el Estado tiene muy poco que hacer al respecto.

Esta misma idea es la que libera el código abierto. En este ámbito las reglas estatales son operativas sólo en la medida en que impongan restricciones que los usuarios quieran adoptar. El Estado puede coordinar la introducción de estándares (como el de «circule por la derecha»), pero ciertamente no puede imponer estándares que restrinjan a los usuarios de modos que éstos no deseen. Esta arquitectura, entonces, constituye un importante mecanismo de control sobre el poder regulador del Estado. El código abierto implica, pues, control abierto —existe el control, pero el usuario es plenamente consciente de él.[27]

El código cerrado funciona de forma diferente. Con él los usuarios no pueden modificar fácilmente los mecanismos de control que vienen insertos en el código. Puede que los hackers y los programadores muy sofisticados sean capaces de hacerlo, pero la mayoría de los usuarios no sabría qué partes se necesitan y qué partes no. O, expresado con más precisión, los usuarios no podrían ver qué partes se requieren y cuáles no debido a que el código fuente no viene incluido con el código cerrado. De esta forma, el código cerrado constituye la mejor estrategia del propagandista —que no introduce ya un capítulo separado que el usuario pueda ignorar, sino una influencia persistente e irreconocible que inclina la historia en la dirección que el propagandista quiere.

Hasta ahora, he manejado a discreción la noción de «usuario», sin precisar que, por más que algunos de estos «usuarios» de Firefox pudieran modificar su código si no les convenciese su modo de funcionar, la inmensa

---

27 Para una discusión que llega a la conclusión opuesta, véase Stephen M. McJohn, «The Paradoxes of Free Software», *George Mason Law Review*, núm. 9, 2000, pp. 25, 64–65. Mathias Strasser extiende el análisis que hago aquí de un modo útil en «A New Paradigm in Intellectual Property Law? The Case Against Open Sources», *Stanford Technology Law Journal*, 2001, p. 4.

mayoría no sería capaz de hacerlo. En consecuencia, para la mayoría de nosotros resulta tan factible modificar el funcionamiento del programa Microsoft Word como hacerlo con el sistema operativo GNU/Linux.

Con todo, la diferencia aquí consiste en que existe —y puede existir legalmente— una comunidad de desarrolladores capaz de modificar el código abierto, pero no existe —ni podría existir legalmente— una comunidad de desarrolladores que modifique el código cerrado, al menos sin el permiso de su propietario. Esa cultura de desarrolladores es el mecanismo crucial que crea la independencia en el seno del código abierto. Sin dicha cultura, existiría muy poca diferencia real entre la regulabilidad del código abierto y del código cerrado.

A su vez, esto implica un tipo diferente de límite sobre este límite de la regulabilidad del código. Así, es probable que las comunidades de desarrolladores propicien ciertas desviaciones de las reglas impuestas por los Estados. En este sentido, es más que probable que dichas comunidades se resistan a la clase de regulación que impusieron los franceses para desbloquear la seguridad de las transacciones financieras, pero es menos probable que inhabiliten los programas antivirus o los filtros de correo basura.

Adónde nos lleva esto

Hasta el momento he hilvanado mi argumentación de un modo sencillo. En respuesta a aquéllos que afirman que es imposible regular la Red, he sostenido que el hecho de que sea o no regulable depende de su arquitectura, de manera que algunas arquitecturas serán regulables y otras no. A continuación, he expuesto cómo el Estado podría influir a la hora de decidir si una arquitectura es o no regulable. Así, el Estado podría tomar medidas tendentes a que una determinada arquitectura pase de ser no regulable a regulable, tanto indirecta (haciendo más rastreable la conducta) como directamente (empleando el código para ejecutar de forma directa el control deseado por el Estado).

El paso final en esta progresión de regulabilidad es una restricción que sólo ahora está volviéndose significativa. El poder estatal para regular el código, para hacer regulable la conducta en el seno del código, depende en

parte de la naturaleza de dicho código: el código abierto es menos regulable que el código cerrado, hasta el punto de que si el código se hace público, el poder del Estado se reduce.

Tomemos como ejemplo la controversia reciente de mayor importancia en el campo del copyright —la compartición de archivos a través de Internet. Tal y como he descrito, esta compartición se basa en una aplicación P2P que funciona en la Red. Las redes de intercambio como StreamCast consisten simplemente en protocolos que ejecutan las aplicaciones P2P. Todos estos protocolos son abiertos y cualquiera puede implementarlos. Y como la tecnología para hacerlo está ampliamente disponible, el hecho de que una compañía concreta decida o no implementar los protocolos no influye en el hecho de que éstos sean implementados —lo que influye es la demanda.

Así pues, imaginémonos por un instante que la industria discográfica lograra finalmente apartar del negocio a todas las compañías que respaldan la compartición de archivos a través de redes P2P. Incluso así, la industria no logrará que ésta deje de existir, y esto porque el código abierto ha permitido que actores no comerciales mantengan la infraestructura de intercambio P2P sin necesidad de contar con la infraestructura comercial.

Obviamente esta afirmación no posee un carácter absoluto. Aquí estoy discutiendo sobre la regulabilidad en términos relativos, no absolutos. Incluso con el código abierto, si el Estado amenaza con castigos suficientemente severos, inducirá un cierto acatamiento de su regulación; e incluso con el código abierto, las técnicas de identificación asociadas a la verificación del código mediante certificados proporcionarían un gran poder al Estado. Por lo tanto, buena parte de la argumentación de la Primera Parte mantiene su vigencia más allá de lo expuesto acerca del código abierto —esto es, si el mundo se vuelve rico en certificados, la regulabilidad seguirá incrementándose. La misma conclusión se derivaría del hecho de que cada vez más código se implante en el hardware en lugar de inscribirse en el software. En este caso, incluso si el código fuera abierto, sería imposible modificarlo.[28]

Sea como fuere, al diseñar una arquitectura para el ciberespacio, los márgenes tienen su importancia. Los principios de un espacio dado no son sólo los de libertad de expresión, autonomía, acceso y privacidad, sino que también puede haber principios relativos al control limitado. Tal y como lo expresa John Perry Barlow, éstos últimos son los principios correspondientes a un

28 Agradezco a Hal Abelson el haberme sugerido esta idea.

cierto «error» que se programa en la arquitectura de la Red —un error que limita el poder del Estado para controlar la Red perfectamente, por más que no anule ese poder por completo.

Para algunos, el objetivo es construir un código que anule cualquier posibilidad de control estatal. Yo no comparto tal objetivo. Ciertamente creo que debe restringirse el poder del Estado, y defiendo las restricciones que el código abierto impone sobre él, pero mi objetivo no es inhabilitar al Estado de forma general. Como ya he planteado, y como quedará claro en la próxima parte, ciertos principios sólo pueden garantizarse si el Estado interviene. Al Estado le queda reservado un papel, por más que éste no sea tan esencial como desearía. Necesitamos comprender cuál es este papel, así como el modo en que nuestros principios podrían apuntalarse en el contexto de la Red.

Con este relato, parece quedar clara una restricción. Tal y como expongo más adelante con mayor exhaustividad, incluso si el código abierto no desactiva por completo el poder regulador del Estado, ciertamente lo modifica. Marginalmente, el código abierto reduce la recompensa derivada de camuflar la regulación en los espacios ocultos del código, operando como una especie de Ley de Libertad de Información (*Freedom of Information Act*) en el contexto de la regulación de la Red. Como sucede con la legislación ordinaria, el código abierto exige que la promulgación de leyes sea pública y, por lo tanto, transparente. En un sentido que George Soros debería comprender, el código abierto constituye un pilar fundamental para construir una sociedad abierta.

Incluso esto supone un importante —algunos dirían fundamental— mecanismo de control sobre el poder del Estado. No obstante, independientemente de que uno esté a favor de la transparencia de manera general, mi propósito hasta ahora se limita a delinear los vínculos. La regulabilidad depende de la naturaleza del código, y el código abierto transforma esta naturaleza. De este modo, el código abierto restringe el poder regulador del Estado —no necesariamente derrotándolo, sino transformándolo.

Tercera parte

Ambigüedades latentes

Hasta ahora, la historia que vengo relatando se ha centrado en la regulación —tanto en la cambiante regulabilidad de la conducta en el ciberespacio (que está aumentando) como en el modo distintivo en que se regulará la conducta en el ciberespacio (a través del código).

En esta Tercera Parte, aplico el análisis trazado hasta el momento a tres áreas de la vida social y política que se verán afectadas por estos cambios —la propiedad intelectual, la privacidad y la libertad de expresión.

En cada una de estas áreas, identificaré qué principios son relevantes y plantearé a continuación cómo se traducen a la vida online. En algunos casos, los principios se trasponen de forma bastante directa, pero en otros se produce lo que en el Capítulo 2 denominé una «ambigüedad latente». Tal ambigüedad nos obliga a elegir entre dos concepciones muy diferentes de los principios que están en juego. Mi objetivo aquí no es realizar esa elección, sino simplemente poner de relieve, al menos, dos opciones.

Asimismo, me planteo otro objetivo en cada uno de los siguientes capítulos. A mi juicio, la lección más importante sobre ciberderecho consiste en la necesidad de que se rindan cuentas del efecto regulador del código. Así, de igual forma que el regulador prudente da cuenta del modo en que el mercado interactúa con la regulación legal, ese regulador

prudente también debe informar del modo en que la tecnología interactúa con dicha regulación legal. A menudo esa interacción es contraria a la intuición, pero a menos que el regulador tome en consideración ese efecto interactivo, su regulación —vaya destinada a controlar la conducta o a proteger ciertas libertades— fracasará.

Sea como fuere, para saber qué principios son relevantes necesitamos un método que los trasponga a un contexto nuevo, por lo que comienzo esta parte con una explicación de dicho método. Los principios que describiré forman parte de nuestra tradición, y han de ser interpretados y dotados de realidad en este contexto. Por lo tanto, comienzo esta parte con un enfoque que ha desarrollado el derecho con el fin de reconocer y respetar tales principios. Se trata de la práctica interpretativa que yo llamo «traducción». Un traductor guarda fidelidad a los compromisos previos. Las ambigüedades latentes son aquellas situaciones en que dicha fidelidad no es aplicable, en que no hay nada a lo que ser fiel porque las opciones a las que nos enfrentamos no fueron planteados a nuestros precursores.[*]

[*] Para una práctica relacionada que se centra más en el contexto de los principios que en su aplicación, véase Andrew L. Shapiro, «The "Principles in Context" Approach to Internet Policymaking», *Columbia Science and Technology Law Review*, núm. 1, 2000, p. 2.

9. Traducción

En el apogeo de una de nuestras «guerras contra las drogas» —la «Ley Seca» que se promulgó en EEUU en la segunda década del siglo XX—, el gobierno federal comenzó a recurrir a una técnica de indagación policial que asustó a muchos, pero que demostró una gran efectividad: el *pinchazo* de teléfonos.[1] Por entonces, la vida había empezado a trasladarse a los cables telefónicos, y en un esfuerzo por sacar partido de las pruebas que pudiera proporcionar este nuevo medio, el gobierno estadounidense comenzó a efectuar escuchas telefónicas sin contar con una orden judicial.

Dado que los propios oficiales de las fuerzas del orden experimentaron un conflicto ético respecto a esta práctica, su empleo se vio bastante limitado. Con todo, la técnica se aplicó para aquellas amenazas percibidas como extremadamente graves, entre las que figuraba el alcohol ilegal, la obsesión de la época.

El más famoso de estos pinchazos fue llevado al Tribunal Supremo en 1928 en el caso «Olmstead contra Estados Unidos». El gobierno federal estaba investigando una de las mayores organizaciones de importación, distribución y venta de bebidas alcohólicas del país. Como parte de la investigación, el gobierno comenzó a pinchar los teléfonos que usaban los contrabandistas y sus agentes. Se trataba de teléfonos privados, pero las interceptaciones siempre se efectuaron sin allanar la propiedad de los investigados,[2] interviniendo las líneas en puntos donde el Gobierno tenía pleno derecho a acceder.

---

1 El propio juez Holmes calificó la intervención de teléfonos como «juego sucio»; *Olmstead vs. United States,* 277 US 438, 470, 1928 (voto particular del juez Oliver Wendell Holmes Jr.).

2 *Ibidem*, p. 457 (el Juez Jefe del Supremo, William H. Taft, estimó que la obtención de las pruebas mediante la intervención de las líneas telefónicas se llevó a cabo sin incurrir en allanamiento, y que, por consiguiente, no violaba la Cuarta Enmienda).

Sirviéndose de esta técnica, el gobierno estadounidense grabó horas y horas de conversaciones (cuya trascripción ocupó 775 folios, según el juez Louis Brandeis),[3] y las empleó para condenar a los acusados en el caso. Éstos cuestionaron el empleo de dichas grabaciones, alegando que el gobierno federal había violado la Constitución para obtenerlas. La Cuarta Enmienda protege «las personas, las casas, los documentos y los efectos personales» contra «registros e incautaciones no razonables» y, tal y como argumentaron los acusados, esta intervención telefónica supuso una violación de su derecho a ser protegidos de registros no razonables.

Conforme a las leyes del momento, estaba claro que para entrar en los domicilios del presunto contrabandista Roy Olmstead y de sus socios y registrarlos (al menos mientras ellos no se encontraran en casa), los investigadores gubernamentales habrían necesitado una orden judicial, es decir, la aprobación de un juez antes de invadir la privacidad de los acusados. Esto es lo que la Cuarta Enmienda había llegado a significar —que ciertos lugares (personas, casas, documentos y efectos personales) gozaban de protección al exigirse una orden cautelar para poder intervenirlos.[4] En este caso no había ninguna orden y, por ende, adujeron los acusados, el registro había sido ilegal y las pruebas derivadas de él tenían que ser desestimadas.

Llegados a este punto, podríamos hacer una pausa e interrogarnos sobre el porqué de esto. Si se lee la Cuarta Enmienda cuidadosamente, resulta difícil discernir en qué casos se exige una orden judicial:

> (a) No se violará el derecho de la gente a que sus personas, casas, documentos y efectos personales estén a salvo de registros e incautaciones no razonables y (b) no se emitirá ninguna orden judicial a menos que esté basada en una causa probable, respaldada por una declaración jurada o un testimonio firme, y que describa detalladamente el lugar donde se efectuará el registro y las personas o cosas que serán incautadas.

---

3 *Ibidem*, p. 471 (voto particular del juez Louis D. Brandeis; los jueces Holmes, Stone y Butler también emitieron votos particulares).

4 Existe un amplio debate acerca del significado original de la Cuarta Enmienda y de cómo ha de aplicarse hoy. Para conocer las dos posiciones enfrentadas, véase Akhil Reed Amar, «Fourth Amendment First Principles», *Harvard Law Review*, núm. 107, 1994, p. 757; Tracey Maclin, «The Complexity of the Fourth Amendment: A Historical Review», *Boston University Law Review*, núm. 77, 1997, p. 925 (criticando el argumento de Amar).

La Cuarta Enmienda contiene en realidad dos mandatos. (He añadido la «a» y la «b» para que se distinga bien la idea). El primero dicta que un determinado derecho (el derecho de la gente a la seguridad) no será violado; el segundo limita las condiciones bajo las cuales se emitirá una orden judicial. Sin embargo, el texto de la Enmienda no establece una relación entre la primera parte y la segunda, y ciertamente no afirma que un registro no sea razonable si no está respaldado por una orden. Así pues, ¿por qué se da la «exigencia de orden judicial»?[5]

Para captar el sentido de esta enmienda, hemos de retroceder hasta el momento en que fue formulada. En aquella época la protección legal contra la invasión de la privacidad era la ley de allanamiento. Si alguien entraba en una propiedad ajena y la desvalijaba, estaba violando los derechos consuetudinarios contra el allanamiento que amparaban a su propietario, el cual podía denunciar al allanador, fuera este un agente de policía o un ciudadano de a pie. La amenaza de tales denuncias daba a la policía un incentivo para no invadir la privacidad ajena.[6]

Incluso sin una orden, sin embargo, un agente de policía que allanara una propiedad podría aducir diferentes argumentos en su defensa, todos ellos centrados en lo «razonable» del registro. Ahora bien, había dos hechos importantes en torno a esta cuestión. En primer lugar, la determinación del carácter razonable del registro correspondía a un jurado, con lo que eran los vecinos e iguales del agente los que juzgaban si su conducta había sido correcta. En segundo lugar, en algunos casos, se consideraba que la determinación de dicho carácter razonable era una cuestión de derecho —es decir, el juez señalaría al jurado que el registro había sido razonable. (Por ejemplo, cuando el agente encontraba material de contrabando en la propiedad del acusado, el registro se consideraba razonable, hubiera o no venido precedido de sospechas suficientes).[7]

---

5 Véase *California vs. Acevedo,* 500 US 565, 582, 1991 (dictamen coincidente del juez Antonin Scalia: el juez describe la exigencia de orden judicial como «repleta de excepciones»).

6 Véase Bradford P. Wilson, «The Fourth Amendment as More Than a Form of Words: The View from the Founding», en Eugene W. Hickok Jr. (ed.), *The Bill of Rights: Original Meaning and Current Understanding*, Charlottesville, University Press of Virginia, 1991, pp. 151, 156–57. Como han señalado muchos autores, en aquella época no existía realmente una «policía» en el sentido en que la entendemos hoy. Las fuerzas policiales modernas son una creación del siglo XIX; véase Carol S. Steiker, «Second Thoughts About First Principles», *Harvard Law Review*, núm. 107, 1994, pp. 820, 830–34; William J. Stuntz, «The Substantive Origins of Criminal Procedure», *Yale Law Journal*, núm. 105, 1995.

7 Véase Amar, «Fourth Amendment First Principles», *op. cit.*, p. 767; Stuntz, «The Substantive Origins of Criminal Procedure», *op. cit.*, p. 400.

Este régimen generaba riesgos obvios para un agente de policía que fuera a registrar la propiedad de alguien. Si la registraba y no encontraba nada, o si un jurado popular estimaba luego que el registro no había sido razonable, debía pagar por su conducta ilegal siendo considerado responsable personal por los derechos que había violado.

Pero el régimen también ofrecía una salvaguarda contra esta responsabilidad —la orden judicial. Si el agente obtenía una orden judicial antes de efectuar el registro, ésta le dotaba de inmunidad ante la acusación de allanamiento. Así, si no encontraba material de contrabando o si su registro resultaba no ser razonable, siempre podría esgrimir la orden judicial para defenderse en caso de ser denunciado.

La creación de incentivos era uno de los objetivos del sistema original. La ley proporcionaba al agente de policía un incentivo para obtener una orden antes de efectuar un registro; si no estaba seguro de lo que iba a encontrar, o si quería evitar arriesgarse a ser denunciado, podía confrontar su criterio consultando a un juez. En cambio, si el agente estaba seguro de lo que iba a hacer, o si deseaba tentar a la suerte, entonces el no contar con una orden judicial no convertía automáticamente su registro en irrazonable. Corría un mayor riesgo de ser considerado responsable legal de los hechos, pero su responsabilidad era todo lo que estaba en juego.

El eslabón débil en este sistema era el juez. Si los jueces eran demasiado laxos, sería muy fácil conseguir una orden judicial,[8] y los jueces débiles constituían una gran preocupación para los defensores de la Cuarta Enmienda. Bajo la dominación británica, los jueces habían sido nombrados por la Corona, y en la época de la Revolución, la Corona era el enemigo. Habiendo sido testigos de demasiados abusos en la emisión de órdenes judiciales, los redactores de la Constitución no estaban dispuestos a conceder a los jueces el control para determinar si los registros gubernamentales eran o no razonables.

En concreto (como describí en el Capítulo 2), los redactores tenían en mente ciertos casos célebres en los que los jueces y el poder ejecutivo habían emitido «órdenes generales» que dotaban a los agentes gubernamentales

---

8 De hecho, como argumenta el profesor William Stuntz de un modo bastante efectivo, un peligro de las órdenes judiciales en general es que los jueces se vuelvan laxos y que, aun así, el producto de su trabajo (la orden) reciba una gran deferencia en los procedimientos subsiguientes; «Warrants and Fourth Amendment Remedies», *Virginia Law Review*, núm. 77, 1991, pp. 881, 893.

del poder para efectuar registros indiscriminados en busca de material de contrabando.[9] Dicho en términos modernos, aquellos registros eran procedimientos «a ciegas» [*fishing expeditions*]. Como los agentes contaban con órdenes judiciales, no podían ser denunciados; como los jueces gozaban de una amplia inmunidad, tampoco podían ser denunciados. En definitiva, como no se podía denunciar a nadie, la tentación de abusar de la ley era grande, y eso era precisamente lo que los redactores de la Cuarta Enmienda querían evitar. Si tenía que existir inmunidad, ésta dimanaría de un jurado popular o de un registro eficaz.

He aquí el origen de la cláusula (b) de la Cuarta Enmienda. Los redactores exigen a los jueces que, al emitir una orden de registro, detallen específicamente «el lugar donde se efectuará el registro y las personas o cosas que serán incautadas», con el propósito de que no puedan emitir órdenes generales. De esta forma, la inmunidad que proporciona la orden estaría limitada a personas y lugares específicos, y a los casos en que existieran indicios fiables para emitir dicha orden.

Este régimen constitucional fue diseñado para lograr un equilibrio entre el interés de las personas en preservar su privacidad y la necesidad legítima del Estado de efectuar registros. El agente de policía tenía un incentivo para conseguir una orden (evitar el riesgo de la responsabilidad personal en caso de ser denunciado); el juez poseía una regla que restringía las condiciones en las que podía emitir una orden; y estas estructuras en su conjunto limitaban las invasiones oficiales de la privacidad a aquellos casos en que existieran motivos fundados para llevarlas a cabo.

Todo esto constituye el trasfondo de la cuestión de los registros. No obstante, fijémonos en lo que sigue.

El régimen original presuponía muchas cosas: la más obvia era la existencia de un sistema de derecho consuetudinario en relación con la ley de allanamiento —era la amenaza de responsabilidad legal derivada de dicha ley la que creaba los incentivos para que los agentes de policía solicitaran órdenes judiciales antes de actuar. Esta presuposición situaba la propiedad en el núcleo de las protecciones originales contempladas en la Constitución estadounidense.

De forma igualmente importante, el régimen presuponía mucho acerca de la tecnología de la época. La Cuarta Enmienda se centra en el allanamiento porque ése era el medio elemental de efectuar un registro por entonces.

---

9 Véase Stuntz, «The Substantive Origins of Criminal Procedure», *op. cit.*, pp. 396–406.

Si hubiera sido posible ver los contenidos de una casa sin entrar en ella, las restricciones de la Cuarta Enmienda habrían tenido poco sentido. Pero las protecciones de dicha enmienda sí que tenían sentido como un modo de lograr un equilibrio entre el poder oficial para registrar y el derecho de la gente a la privacidad, todo ello en el contexto del régimen legal de allanamiento y de las tecnologías invasoras de la privacidad que prevalecían a finales del siglo XVIII.

Ahora bien, las presuposiciones —aquello que se da por sentado o se considera fuera de discusión— varían.[10] ¿Cómo hemos de responder cuando esto ocurre? ¿Cómo leemos un texto redactado con el trasfondo de ciertas presuposiciones cuando éstas ya no son aplicables?

En EEUU, o en cualquier nación con una Constitución de unos doscientos años de antigüedad, éste es el problema central de la interpretación constitucional. ¿Qué sucedería, por ejemplo, si los gobiernos estatales optaran simplemente por abolir los derechos ciudadanos contra el allanamiento de morada? ¿Habría alguna diferencia en la interpretación de la Cuarta Enmienda?[11] ¿Que sucedería si las tecnologías de registro cambiaran tan repentinamente que nunca más se necesitara entrar en la propiedad ajena para saber lo que se guarda en ella? ¿Debería interpretarse la Cuarta Enmienda de modo diferente en ese caso?

Pese a que la historia del tratamiento que el Tribunal Supremo ha dado a estas cuestiones carece de un patrón perfectamente definido, podemos identificar dos estrategias distintas que compiten por la atención de dicho tribunal. Una se centra en lo que los redactores o fundadores habrían hecho —la estrategia del «originalismo literal» [*one-step originalism*]; la otra trata de hallar una lectura actual de la Constitución original que mantenga su significado en el contexto presente —una estrategia que denomino traducción.

Ambas estrategias están presentes en el caso «Olmstead contra Estados Unidos». Cuando el gobierno federal pinchó los teléfonos de los acusados sin orden judicial, el Tribunal Supremo tenía que decidir si el uso de esta clase de pruebas era admisible o coherente con los principios de la Cuarta Enmienda. Los acusados adujeron que el gobierno estadounidense debía obtener una orden judicial para intervenir los teléfonos, y éste replicó que la Cuarta Enmienda simplemente no era aplicable en este caso.

---

10 Véase *United States vs. Virginia,* 518 US 515, 566–567, 1996 (voto particular del juez Antonin Scalia: «Eran muy cerrados de mente —toda época lo es [...] con respecto a los asuntos sobre los que no puede pensar simplemente porque no se los considera objeto de debate»).

11 Véase Lawrence Lessig, «Fidelity in Translation», *Texas Law Review*, núm. 71, 1993, pp. 1165, 1230.

La argumentación gubernamental era muy sencilla. La Cuarta Enmienda presuponía que el registro gubernamental incurriría en allanamiento, y se ocupaba de regular las condiciones en las que los agentes de policía podían allanar una propiedad. No obstante, como la intervención telefónica constituía una invasión de privacidad sin allanamiento, el gobierno federal podía pinchar los teléfonos de los acusados sin entrar en su propiedad, con lo que la Cuarta Enmienda no era de aplicación en este caso. Las invasiones de privacidad que no conllevaban allanamiento simplemente quedaban fuera del ámbito de aplicación de dicha enmienda.

El Tribunal Supremo se mostró de acuerdo con esta argumentación. En un dictamen escrito por el juez jefe (y antiguo presidente) William Howard Taft, el Supremo dio la razón al gobierno de EEUU.

> La enmienda no prohíbe lo que se hizo aquí. No hubo registro. No hubo incautación. Las pruebas se obtuvieron sólo y exclusivamente mediante el uso del sentido auditivo. El lenguaje de la enmienda no puede extenderse y expandirse para incluir las líneas telefónicas que llegan al mundo entero desde la casa o la oficina del acusado.[12]

Esta conclusión fue recibida con sorpresa y conmoción. En aquel momento buena parte de la vida se había trasladado ya a las líneas telefónicas. La gente comenzaba a comprender lo que significaba tener un contacto personal *online*, y contaban con que el sistema telefónico protegiera sus secretos íntimos. De hecho, las compañías telefónicas, tras luchar fuertemente contra la autoridad que reclamaba para sí el gobierno estadounidense, se comprometieron a no colaborar a menos que así lo exigiera la ley.[13] A pesar de esta resistencia, el Supremo concluyó que la Constitución no interfería en invasiones de privacidad de esta naturaleza. No lo habría hecho en la época en que fue redactada, y tampoco lo haría a la hora de emitir un veredicto sobre este caso.

No obstante, el voto particular emitido por el juez Brandeis (también emitieron votos particulares los jueces Holmes, Stone y Butler) sostenía un punto de vista diferente. Al igual que en el dictamen de Taft, la cuestión central era la fidelidad, si bien esta se concebía de forma bastante diferente.

---

12 *Olmstead vs. United States*, 277 US 438, 470, 1928, pp. 464–465.

13 *Ibidem*, escrito para la Pacific Telephone & Telegraph Company (nos. 493, 532, 533).

Brandeis reconoció que la Cuarta Enmienda, en su redacción original, sólo se aplicaba al allanamiento de morada,[14] pero arguyó que era así porque en la época en que fue redactada, el allanamiento era la única tecnología de invasión de la privacidad. Ésa era la presuposición de sus redactores, pero tal presuposición ya había variado. Dada esta variación, sostuvo Brandeis, sobre el Supremo recaía la responsabilidad de interpretar la enmienda de un modo que mantuviera intacto su significado, independientemente de la modificación de las circunstancias. Así pues, el objetivo debía ser traducir las protecciones originales a un contexto en que la tecnología para invadir la privacidad había variado.[15] Y esto se lograría, concluyó Brandeis, aplicando las protecciones consagradas en la Cuarta Enmienda a aquellas invasiones que no constituían propiamente allanamientos.

Estas dos posturas marcan dos modos diferentes de interpretación constitucional. Mientras que el juez Taft halla la fidelidad limitándose a repetir lo que establecieron los redactores de la Constitución, el juez Brandeis la encuentra en su equivalente actual. Si adoptáramos la tesis de Taft, afirmaba Brandeis, suprimiríamos la protección de la privacidad que los redactores consagraron originalmente; si adoptáramos la tesis de Brandeis, insinuaba Taft, estaríamos añadiendo a la Constitución algo que los redactores no habían escrito.

---

14 *Ibidem*, p. 473 (voto particular del juez Louis Brandeis).

15 «Traducción» no es el término que emplea Brandeis, aunque sí que constituye un término jurídico. El juez Robert H. Jackson captura mejor esta idea en *West Virginia State Board of Education vs. Barnette,* 319 US 624, 639–40, 1943: «Nuestro deber de aplicar la Declaración de Derechos a las aseveraciones de la autoridad oficial tampoco depende de nuestra posesión de una marcada competencia en el ámbito en el que se produce la violación de esos derechos. Ciertamente la tarea de traducir las majestuosas generalidades de la Declaración de Derechos, concebida como parte del patrón de gobierno liberal en el siglo XVIII, en restricciones concretas sobre funcionarios que se ocupan de los problemas del siglo XX, perturba nuestra confianza en nosotros mismos. Estos principios crecieron en un terreno que también produjo una filosofía que defendía que el individuo era el centro de la sociedad, que su libertad era alcanzable mediante la mera ausencia de restricciones estatales, y que al Estado debían confiársele pocos medios de control y sólo una levísima supervisión de los asuntos de los ciudadanos. Ahora hemos de transplantar tales derechos a un suelo donde el concepto del *laissez-faire* o principio de no interferencia ha languidecido, al menos con respecto a los asuntos económicos, y donde los avances sociales se persiguen cada vez más por medio de una mayor integración social y de mecanismos de control estatal amplios y sólidos. Este cambio de condiciones a menudo nos priva de precedentes fiables y nos deja más de lo que desearíamos a merced de nuestros propios juicios. Pero, en estas cuestiones, actuamos no por la autoridad de nuestra competencia, sino por la fuerza de nuestro cometido. No podemos, apoyándonos en estimaciones modestas de nuestra competencia en especialidades como la educación pública, aplazar la resolución judicial que la historia reconoce como la función de este tribunal cuando se infringe la libertad».

Los partidarios de una y otra postura alegaban que la opinión de los otros habría «modificado» el significado de la Constitución. Ahora bien, ¿cuál de las dos posturas, la del Tribunal Supremo o la del juez Brandeis, «modificaría» realmente el significado de la Cuarta Enmienda?

Para responder a esta pregunta, hemos de preguntarnos en primer lugar: ¿«modificar» respecto a qué? ¿Cuál es la referencia con respecto a la cual un cambio es un cambio? Ciertamente Brandeis habría estado de acuerdo en que, en 1791, cualquier fallo del Tribunal Supremo que interpretara que la recién promulgada enmienda abarcaba más allá del allanamiento habría sido incorrecto. Sin embargo, cuando algo que la enmienda original presuponía ha sufrido una variación, ¿está tan claro que la respuesta correcta del Supremo es la de actuar como si nada en absoluto hubiera cambiado?

El método de Brandeis tenía en cuenta la variación de la presuposición. Este juez ofrecía una interpretación que modificaba el alcance de la enmienda con el fin de mantener la protección de la privacidad que ella garantizaba. Por su parte, Taft ofrecía una interpretación que mantenía el alcance de la enmienda pero modificaba su protección de la privacidad. Cada interpretación dejaba un elemento constante y, a la vez, modificaba otro. La pregunta es entonces: ¿qué interpretación mantenía lo que el criterio de fidelidad a la Constitución demandaba?

Podríamos captar mejor el fondo de la cuestión por medio de una recreación un tanto estilizada. Imaginémonos que fuera posible cuantificar la privacidad; de esa manera podríamos describir la modificación en la cantidad de privacidad que cualquier cambio tecnológico conlleva. (Robert Post nos ha proporcionado un argumento absolutamente persuasivo acerca de por qué la privacidad no es cuantificable, pero mi finalidad aquí es meramente ilustrativa).[16] En este sentido, imaginémonos que en 1791 la protección contra el allanamiento físico protegiera el 90 % de la privacidad personal. Los agentes del Estado seguían pudiendo estar en la calle y escuchar a través de las ventanas que se dejaran abiertas, pero, con todo, la invasión de la privacidad que representaba esa amenaza era bastante reducida. En definitiva, un régimen que protegiera a los ciudadanos contra el allanamiento protegía también su privacidad de forma casi completa.

---

16 Véase Robert Post, *Constitutional Domains: Democracy, Community, Management*, Cambridge (Mass.), Harvard University Press, 1995, pp. 60–64.

Cuando aparecieron los teléfonos, sin embargo, esta protección varió. Una gran cantidad de información privada fue vertida a través de las líneas telefónicas. En esta situación, si el pinchazo de teléfonos no era considerado allanamiento, mucha menos porción de vida privada quedaría a salvo del fisgoneo estatal, con lo que la Cuarta Enmienda pasaría de proteger el 90 % de la privacidad personal a proteger sólo el 50 %.

El juez Brandeis quería interpretar esta enmienda de modo que siguiera protegiendo ese 90 % de privacidad que protegía originalmente —aunque ello exigiera que la enmienda protegiera contra algo más que el mero allanamiento de morada. Podríamos afirmar que quería interpretarla de forma diferente para que continuara protegiendo lo mismo.

Esta forma de argumentación es habitual en la historia constitucional de EEUU, y constituye un aspecto esencial de lo mejor de nuestra tradición constitucional.[17] Es una argumentación que responde a la modificación de las circunstancias proponiendo una interpretación que neutraliza estas modificaciones y mantiene el significado original. Es, además, una argumentación que invocan tanto jueces de derecha como de izquierda,[18] y es una vía para mantener viva una disposición constitucional —para asegurarse de que los cambios en el mundo no alteran el significado del texto constitucional. Podemos afirmar que es una argumentación que busca traducir las protecciones que la Cuarta Enmienda introdujo en 1791 de modo que se mantenga el mismo conjunto de protecciones en cualquier otro momento posterior de nuestra historia. Para ello, se asume que el Tribunal Supremo puede tener que interpretar la enmienda de forma diferente, pero esto no implica ni mejorarla ni incorporar nuevas protecciones. Lo que implica esta interpretación diferente es la acomodación de los cambios en la protección que han resultado de los cambios tecnológicos. Se trata, pues, de traducir para mantener intacto el significado.

---

17 Véase Lessig, «Fidelity in Translation», *op. cit.*, pp. 1214–68; Lawrence Lessig, «Translating Federalism: United States vs. Lopez», *Supreme Court Review*, 1995, pp. 125, 146. Para un análisis más sofisticado de cómo los cambios tecnológicos en el contexto de las telecomunicaciones están afectando a la legislación y a la doctrina judicial, véase Monroe E. Price y John F. Duffy, «Technological Change and Doctrinal Persistence: Telecommunications Reformin Congress and the Court», *Columbia Law Review*, núm. 97, 1997, p. 976.

18 Así, por ejemplo, las traducciones que respaldan el federalismo son traducciones de la derecha, mientras que las que respaldan los derechos en procedimientos criminales son traducciones de izquierdas.

Si existe un juez que merezca el elogio del ciberespacio, si existe un dictamen del Tribunal Supremo que debiera convertirse en el modelo de los ciberactivistas del futuro, y si se ha escrito un primer capítulo en la batalla para proteger el ciberespacio, ésos son este juez, este dictamen y este caso. Brandeis nos brindó un modelo de interpretación de la Constitución que mantiene su significado y sus valores a través de diferentes épocas y contextos. Es un método que reconoce lo que ha cambiado y acomoda tal cambio para mantener algo que los redactores de la Carta Magna nos otorgaron originalmente. Es un método que traduce el significado de la Constitución a través de contextos fundamentalmente diferentes —por más que entre ellos medie tanta distancia como la que nos separa a nosotros de los redactores, o al ciberespacio del espacio real.

No obstante, fue el dictamen del juez Taft el que sentó jurisprudencia, y fue su estrecha visión de la Cuarta Enmienda la que acabó prevaleciendo. Tuvieron que transcurrir cuarenta años para que el Tribunal Supremo adoptara la interpretación de la Cuarta Enmienda del juez Brandeis —cuarenta años hasta que se anuló la sentencia del caso «Olmstead contra Estados Unidos». El caso que propició esta anulación fue «Katz contra Estados Unidos».[19]

Charles Katz era sospechoso de transmitir telefónicamente información sobre apuestas a clientes de otros estados. Los agentes federales grabaron varias de sus transmisiones telefónicas incorporando un dispositivo de escucha en el exterior de una cabina telefónica desde donde realizaba sus llamadas. Katz fue acusado a partir de las pruebas así obtenidas, y el tribunal de apelación ratificó la condena basándose en el caso «Olmstead contra Estados Unidos».

Laurence Tribe, profesor de la Facultad de Derecho de Harvard, tomó parte en aquel caso en los comienzos de su carrera legal:

> Como secretario del juez del Tribunal Supremo Potter Stewart, me encontré trabajando en un caso vinculado con la vigilancia electrónica por parte del Estado de un presunto delincuente por medio de un dispositivo minúsculo incorporado al exterior de una cabina telefónica. Dado que la invasión de la privacidad del sospechoso se llevó a cabo sin allanamiento físico de un «área constitucionalmente protegida», el gobierno federal arguyó, apoyándose en la jurisprudencia que sentó el caso «Olmstead contra Estados Unidos», que no se había producido ni «registro» ni «incautación» y que, por consiguiente, el «derecho de la gente de que sus personas, casas, documentos y efectos personales estén a salvo de registros e incautaciones no razonables» que consagra la Cuarta Enmienda simplemente no era aplicable en este caso.

---

19 *Katz vs. United States,* 389 US 347, 353, 1967.

> Al principio, sólo se emitieron cuatro votos favorables a anular la sentencia del caso «Olmstead contra Estados Unidos» y a sostener la aplicabilidad de la Cuarta Enmienda a las intervenciones telefónicas y a las escuchas electrónicas. Me enorgullece afirmar que, siendo sólo un chico de veintiséis años, tuve que ver al menos un poquito con que ese número pasara de cuatro a siete —y con la interpretación, adoptada formalmente por una mayoría de siete jueces en diciembre de 1967, de que la Cuarta Enmienda «protege a las personas, no a los lugares» [389 US en 351]. En esa decisión, «Katz contra Estados Unidos», el Tribunal Supremo finalmente rechazó la doctrina Olmstead y las muchas decisiones que se habían apoyado sobre ella, razonando que, dado el papel que estaban adquiriendo las telecomunicaciones electrónicas en la vida moderna, la finalidad [de la Primera Enmienda] de proteger la libertad de expresión, así como la finalidad [de la Cuarta Enmienda] de proteger la privacidad exigían tratar como un «registro» cualquier invasión de las comunicaciones telefónicas confidenciales de una persona, existiera o no allanamiento físico.[20]

En «Katz contra Estados Unidos», el Tribunal Supremo adoptó la tesis de Brandeis en lugar de la de Taft. Buscó una interpretación de la Cuarta Enmienda que mantuviera su sentido en un contexto distinto. En el contexto de 1791 en que vivieron los redactores, la protección contra el allanamiento de morada era un modo efectivo de proteger contra la invasión de la privacidad, pero no lo era en el contexto de Katz de los años sesenta del siglo XX. En ese momento buena parte de la vida íntima transcurría en lugares a los que no llegaban las reglas de propiedad (por ejemplo, en el «éter» de la red telefónica de AT&T), por lo que un régimen que hiciera depender la privacidad de la propiedad no protegía aquélla en la misma medida en que lo habían pretendido los redactores de la Constitución. Así pues, en «Katz contra Estados Unidos» el juez Stewart buscó remediar esto vinculando la Cuarta Enmienda a una protección más directa de la privacidad.

El vínculo era la idea de «una expectativa razonable de privacidad». El valor fundamental, escribió el juez Stewart, consistía en proteger «a las personas, no a los lugares».[21] En consecuencia, la técnica fundamental debería ser la de proteger a las personas allá donde éstas tuvieran una expectativa razonable de privacidad. En estos casos, el Estado no puede invadir ese espacio de privacidad sin satisfacer los requisitos establecidos en la Cuarta Enmienda.

---

20 Laurence H. Tribe, «The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier», intervención en el Primer Congreso sobre Ordenadores, Libertad y Privacidad, 26 de marzo de 1991, reimpresa en *The Humanist*, septiembre-octubre de 1991, pp. 15, 20–21.

21 *Katz vs. United States,* 389 US 347, 351, 1967.

Hay mucho que admirar en el dictamen del juez Stewart, al menos en la medida en que demuestra su voluntad de conformar herramientas que mantengan el significado de la Constitución en circunstancias que han variado —o, insisto, en la medida en que trata de traducir las protecciones de la Cuarta Enmienda a un contexto moderno. Y también hay mucho que cuestionar en su dictamen.[22] No obstante, podemos dejar de lado estas cuestiones por el momento para centrarnos en un aspecto del problema que normalmente está fuera de la discusión.

Por más que sea difícil trazar los contornos de la cuestión, al menos está claro que los redactores de la Constitución tomaron una decisión consciente para proteger la privacidad. No se trató, pues, de un asunto ajeno a su discusión original o que se les pasara por alto, ni tampoco se trata del «derecho a la privacidad» del que se quejan los conservadores en el contexto del derecho al aborto. Estamos hablando del derecho a vivir libres de la intrusión estatal en el «santuario» que constituye un hogar privado. Las amenazas estatales a la privacidad personal estaban en el centro del movimiento que condujo a la república estadounidense; los jueces Brandeis y Stewart simplemente trataron de hacer efectiva esa decisión en contextos donde la estructura original había perdido su efectividad.

Este tipo de traducciones están presididas por la honestidad. Los principios originales por los que se opta están bastante claros, el modo en que los contextos socavan su aplicación original es bastante fácil de comprender, y las interpretaciones que restaurarían los principios originales resultan bastante obvias. Por supuesto, casos como éstos exigen a menudo un determinado coraje interpretativo —una voluntad de mantener la fidelidad interpretativa mediante el cambio de una práctica de interpretación—, pero al menos la dirección está clara, por más que los medios sean un poco burdos.[23]

---

22 Tal y como atestiguará la historia de la protección de la Cuarta Enmienda a partir del caso «Katz contra Estados Unidos», la técnica empleada por el juez Stewart resultó finalmente bastante ineficaz. No cabe duda de que el alcance de la Cuarta Enmienda era limitado en cuanto que estaba ligado a nociones de propiedad, pero, al menos, llegaba tan lejos como lo hacía el alcance de la propiedad. Se podía resistir a las presiones, dado que la «propiedad» tiene un cuerpo de leyes independiente de las cuestiones de privacidad. Pero, una vez que el Supremo adoptó la prueba de la «expectativa razonable de privacidad», pudo restringir luego estas «expectativas razonables» en el contexto de la Cuarta Enmienda, con escasas consecuencias fuera de ese contexto. El resultado de todo esto ha sido un alcance cada vez más reducido de la protección de la privacidad.

23 Véase Lessig, «Translating Federalism», *op. cit.*, pp. 206–211.

Éstos son los casos fáciles, que resultan aún más fáciles cuando no tratamos de trasponer los principios de un pasado distante al futuro, sino simplemente de un contexto a otro distinto. Cuando sabemos qué principios queremos mantener, sólo necesitamos ser creativos para encontrar el modo de hacerlo.

El ciberespacio nos planteará muchos de estos casos fáciles. Cuando los tribunales se enfrenten a ellos, deberían seguir el ejemplo del juez Brandeis: deberían optar por la traducción e instar al Tribunal Supremo a hacer lo mismo. En aquellos casos en que las circunstancias hayan variado hasta el punto de anular las protecciones de algún derecho original, el Supremo debería adoptar una interpretación de la Constitución que restaure ese derecho.

Ahora bien, algunos casos no resultarán tan fáciles. Unas veces no se podrá optar por la traducción, otras veces la traducción remitirá a principios que ya no deseamos mantener, y otras veces no podremos determinar qué principios debería escoger la traducción. Éste era el problema que nos planteaba el gusano del Capítulo 2 y que nos llevaba a la cuestión de las ambigüedades latentes. Y es que, en ocasiones, el cambio de contexto revela una ambigüedad latente en el contexto original, en cuyo caso hemos de escoger entre dos principios diferentes, cada uno de los cuales podría considerarse coherente con el principio original. Puesto que ambas opciones podrían aparecer como correctas, no podemos afirmar cuál se primaba en el contexto original (sea actual o de hace doscientos años).

El profesor Tribe describe un ejemplo de lo anterior en un artículo fundamental en el campo del ciberderecho, «The Constitution in Cyberspace» («La Constitución en el ciberespacio»).[24] En él, Tribe bosqueja un método de interpretación de la Constitución en el ciberespacio que trata de hacerla «tecnológicamente neutral». El objetivo es adoptar interpretaciones (o quizá incluso una enmienda) que dejen claro que las transformaciones tecnológicas no van a modificar el significado de la Constitución. Así pues, siempre debemos adoptar interpretaciones de la Constitución que mantengan sus principios originales. Cuando los jueces se ocupen de asuntos relacionados con el ciberespacio, han de actuar como traductores: las diferentes tecnologías constituyen lenguajes distintos, y el objetivo es encontrar una interpretación de la Constitución que mantenga intacto su significado al margen de las tecnologías que existan en un mundo o en otro.[25]

---

24 Tribe, «The Constitution in Cyberspace», *op. cit.*, p. 15.

25 Véase Lawrence Lessig, «Reading the Constitution in Cyberspace», *Emory Law Journal*, núm. 45, 1996, pp. 869, 872.

En esto radica la fidelidad de la traducción. Sin embargo, este tipo de traducción se expresa como si se limitara a transferir a otro contexto algo que ya se ha dicho. Oculta la creatividad que encierra su acto, finge una cierta deferencia educada o respetuosa. Esta forma de interpretar la Constitución insiste en que las decisiones políticas importantes ya se han tomado con anterioridad, y que todo lo que se requiere es una especie de ajuste técnico. Así pues, su objetivo es mantener afinado el piano mientras se lo traslada de una sala de conciertos a otra.

Pero entonces el profesor Tribe ofrece un ejemplo que puede hacer que este método parezca vacuo. La cuestión está relacionada con el significado de la «cláusula de confrontación» de la Sexta Enmienda —el derecho del encausado a «ser confrontado con los testigos de la acusación»—, y lleva a Tribe a preguntarse: ¿cómo deberíamos interpretar esta cláusula hoy?

En la época de los redactores de la Constitución, explica Tribe, la tecnología de confrontación era muy simple —el careo bidireccional. Si un testigo se confrontaba con el acusado, a su vez éste se confrontaba con aquél necesariamente. Se trataba de una necesidad que venía impuesta por la tecnología de la época, pero hoy es posible que la confrontación sea unidireccional —el testigo se confronta con el acusado, pero éste no tiene que confrontarse con el testigo. La cuestión entonces es si la cláusula de la confrontación exige que esta sea unidireccional o bidireccional.[26]

Concedamos que las descripciones que el profesor Tribe realiza de las tecnologías disponibles son correctas, y que los fundadores adoptaron la única cláusula de confrontación que la tecnología de la época posibilitaba. La auténtica pregunta viene a continuación: ahora que la tecnología permite dos posibilidades —la confrontación unidireccional o bidireccional—, ¿qué exige la Constitución?

La respuesta del Tribunal Supremo en su decisión de 1990 relativa al caso «El Estado de Maryland contra Craig» fue muy clara: la Constitución exige únicamente la confrontación unidireccional. Un régimen que interprete que la cláusula de confrontación permite sólo el careo unidireccional, al menos cuando existan fuertes intereses para no exigir que sea bidireccional, supone una traducción correcta de la cláusula original.[27]

---

26 Este ejemplo está extraído de *Maryland vs. Craig*, 497 US 836, 1990.

27 Véase Tribe, «The Constitution in Cyberspace», *op. cit.*, p. 15.

En tanto que opción política, esta respuesta ciertamente me agrada, pero no logro percibir cuál es su fuente jurídica. Me parece que estamos ante una cuestión que los redactores de la Constitución no dejaron decidida, y sobre la que bien podrían no haberse puesto de acuerdo si se les hubiera presentado en su momento. Dada la tecnología de 1791, no tuvieron que decidir entre la confrontación unidireccional y la bidireccional; dado el conflicto entre los principios que están en juego, no es obvio determinar cómo habrían tomado su decisión. En consecuencia, hablar como si los redactores nos hubieran proporcionado una respuesta sobre esta cuestión resulta un poco engañoso. En este caso los redactores no nos dieron ninguna respuesta y, a mi juicio, no se puede extraer ninguna respuesta de lo que dijeron.

Como el gusano del Capítulo 2, la cláusula de confrontación nos plantea una ambigüedad latente.[28] La aplicación al ciberespacio del Derecho Constitucional nos revelará muchas más ambigüedades latentes, las cuales nos colocan ante una decisión: ¿cómo seguiremos adelante en este nuevo ámbito?

Esta situación no es algo terrible: no supone ningún desastre tener que tomar una decisión —siempre que seamos capaces de hacerlo. Pero es aquí justamente donde se encuentra el quid de la cuestión a mi entender. Como tendré ocasión de exponer con más detalle en la Cuarta Parte, dadas las actitudes actuales de nuestros tribunales y nuestra cultura legal en general, las decisiones constitucionales salen caras. Somos malos tomándolas y no parece probable que a corto plazo mejoremos en este sentido.

Cuando no existe una respuesta acerca de cómo proceder —cuando la traducción deja abierta alguna incógnita—, disponemos de dos tipos de respuestas en la práctica constitucional. Una de ellas es pasiva: los tribunales se limitan a dejar que sea el poder legislativo el que decida. Ésta es la respuesta que el juez Scalia defiende en el contexto de la Decimocuarta Enmienda. En asuntos que quedaron «fuera de debate» para los redactores de la Constitución, ésta no se pronuncia.[29] En este caso, sólo el poder legislativo puede plantear cuestiones relativas a principios constitucionales y, por consiguiente, establecer qué dirá la Constitución.

---

28 «Una ambigüedad latente surge de hechos triviales o colaterales que vuelven incierto el significado de un elemento escrito aunque su lenguaje sea claro e inequívoco. El típico ejemplo de ambigüedad es aquél en que un escrito se refiere a una persona o cosa concreta y, por lo tanto, es aparentemente claro en su literalidad, pero, al ser aplicado a objetos externos, encontramos que se ajusta de la misma forma a dos o más de ellos»; Walter H. E. Jaeger (ed.), *Williston on Contracts* (3ª), Mount Kisco (NY), Baker Voorhis, 1957, pp. 627, 898.

29 Véase *United States vs. Virginia,* 518 US 515, 566–67, 1996 (voto particular del juez Antonin Scalia).

La segunda respuesta es más activa: los tribunales hallan un modo de articular los principios constitucionales que no estaban presentes en el momento de la redacción. Dichos tribunales contribuyen a estimular una discusión en torno a estos principios fundamentales —o, al menos, se unen a la discusión— con el fin de centrar un debate que, en última instancia, pueda resolverse en otro lugar. La primera respuesta es una manera de no hacer nada, mientras que la segunda es una manera de alentar un diálogo sobre los principios constitucionales con el fin de afrontar y resolver nuevas cuestiones.[30]

Mi temor con respecto al ciberespacio es que respondamos de la primera manera —que los tribunales, las instituciones que tienen la mayor responsabilidad de articular los principios constitucionales, se inhiban ante asuntos de relevancia constitucional y dejen que el poder legislativo decida sobre ellos. A mi juicio, los tribunales se inhibirán en estos casos porque, como defiendo en lo que queda de este libro, sienten que las cuestiones que ha suscitado el ciberespacio son nuevas y, por consiguiente, presentan matices políticos. Y cuando una cuestión presenta un matiz político, los tribunales se abstienen de resolverla.

Si me inclino por esta opción, no es porque tema al poder legislativo, sino porque el nivel de discurso constitucional entre los miembros del legislativo es muy exiguo en nuestros días. El filósofo Bernard Williams ha justificado esta dejadez legislativa basándose en el papel tan central que ha asumido el Tribunal Supremo en la articulación de los valores constitucionales.[31] Tenga o no razón Williams, hay algo que está meridianamente claro: el nivel de discurso constitucional de nuestro actual Congreso está muy por debajo del nivel al que debería estar para tratar las cuestiones relacionadas con los principios constitucionales que suscitará el ciberespacio.

No está claro cómo podremos superar esta pobreza de discurso constitucional. El pensamiento constitucional ha sido durante demasiado tiempo dominio exclusivo de abogados y jueces, de forma que hemos quedado atrapados por un modo de razonar que finge que todas las preguntas importantes ya han sido respondidas, y que nuestra tarea actual se limita a traducir dichas respuestas a los nuevos tiempos. De resultas, no sabemos bien cómo

---

30 Se han producido trabajos relacionados bajo la denominación de «Nuevo Minimalismo Judicial». Véase Christopher J. Peters y Neal Devins, «Alexander Bickel and the New Judicial Minimalism», en Kenneth D. Ward y Cecilia R. Castillo (eds.), *The Judiciary and American Democracy*, Albany, State University of New York Press, 2005.

31 Véase Bernard Williams, «The Relations of Philosophy to the Professions and Public Life», manuscrito inédito.

proceder cuando nos damos cuenta de que no todas las respuestas están dadas. Ahora que las naciones de todo el mundo luchan por expresar y adoptar principios constitucionales, la nuestra, EEUU, que posee la tradición constitucional más longeva, ha perdido la práctica de adoptar, articular y decidir acerca de dichos principios.

Volveré sobre este problema en el Capítulo 15. Por ahora, mi propósito es meramente descriptivo. La traducción constituye un modo de afrontar las encrucijadas que plantea el ciberespacio, un modo de hallar la equivalencia entre diferentes contextos. Ahora bien, en las cuatro aplicaciones que vienen a continuación, lanzaré estas preguntas: ¿es suficiente el pasado? ¿Existen decisiones que los redactores de la Constitución no abordaron en su momento? ¿Son decisiones que nosotros hemos de tomar ahora?[32]

32 Para un argumento sólido en contra de que la revisión judicial desempeñe un papel importante en asuntos como éste, véase Orin Kerr, «The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution», *Michigan Law Review*, núm. 102, marzo de 2004, p. 801.

10. Propiedad Intelectual

Harold Reeves es uno de los mejores ayudantes de investigación que he tenido. (Lamentablemente, el mundo del Derecho le perdió —¡se hizo sacerdote!). Al comienzo de su segundo año en la Facultad de Derecho de la Universidad de Chicago, se me acercó con una idea que se le había ocurrido para un artículo —que sería publicado en la revista de la Facultad.[1] El tema del artículo era la ley de allanamiento en el ciberespacio –en qué casos y cómo debía protegerse a los «propietarios de espacio» del tipo de intrusiones contra las que la Cuarta Enmienda protege en el espacio real. Su idea inicial era simple: no debía existir ley de allanamiento en el ciberespacio.[2] El Derecho no debería conceder a los «propietarios de espacio» ninguna protección legal contra la invasión en el ciberespacio, sino que debía obligarles a arreglárselas solos.

La idea de Reeves era un poco alocada y, a fin de cuentas, creo que era errónea.[3] Ahora bien, contenía una visión bastante brillante que debería ser central a la hora de pensar sobre el ciberderecho.

---

1 Harold Smith Reeves, «Property in Cyberspace», *University of Chicago Law Review*, núm. 63, 1996, p. 761.

2 Esta no fue la conclusión a la que llegó finalmente. En lugar de ello, Reeves concluyó, no que no deberían protegerse los límites en el ciberespacio, sino que la naturaleza poco convencional del ciberespacio exige establecer estos límites según líneas no tradicionales, específicas del contexto. Esta conclusión, afirma Reeves, requiere que el Derecho comprenda tanto el entorno del ciberespacio como los intereses de aquéllos que efectúan transacciones en él; véase *ibidem*, p. 799.

3 Cf. Yochai Benkler, «Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain», *New York University Law Review*, núm. 74, 1999, p. 354.

La idea —presentada de un modo mucho más breve y mucho menos elegante de como lo hizo Reeves— es ésta: la pregunta que debe plantear el Derecho es qué medios proporcionarían el conjunto más eficaz de protecciones para los intereses de la propiedad en el ciberespacio. Hay dos tipos posibles de protección. Una es la protección legal tradicional —por la que la ley define un espacio donde los demás no deben entrar y castiga a aquéllos que lo hacen pese a todo. La otra protección es una valla, un dispositivo tecnológico (un fragmento de código) que (entre otras cosas) bloquea la entrada a los no deseados. En el espacio real, por supuesto, disponemos de ambos tipos de protección —la ley de allanamiento y las vallas que la complementan. Ambas cuestan dinero y el beneficio de cada una de ellas no es necesariamente el mismo. Desde una perspectiva social, desearíamos adoptar la combinación de ley y vallas que proporcionara la protección más óptima al menor coste. (Expresado en términos económicos, desearíamos una combinación tal que el coste marginal de una unidad de protección adicional equivaliese al beneficio marginal derivado de ella).

La implicación que tiene esta idea en el espacio real es que en ocasiones tiene sentido hacer recaer el coste de la protección en los ciudadanos, en vez de en el Estado. Así, por ejemplo, si un granjero desea almacenar semillas de gran valor en una parte remota de su granja, le conviene más asumir el coste de protegerlas mediante vallas que requerir que la policía patrulle la zona más meticulosamente o que castigue con mayor dureza a los ladrones que atrape. Siempre se trata de una cuestión de equilibrio entre los costes y los beneficios de la protección privada y de la estatal.

La visión de Reeves acerca del ciberespacio sigue la misma línea. La potección óptima para los espacios del ciberespacio surge de la combinación de ley pública y vallas privadas. Lo que hemos de preguntarnos a la hora de determinar dicha combinación es qué protección implica unos costes marginales menores. Reeves sostiene que los costes de la ley en este contexto son extremadamente altos —en parte debido a los costes de su aplicación, pero también porque a la ley le resulta difícil distinguir entre usos legítimos e ilegítimos en el ciberespacio. Existen muchos «agentes» que podrían «usar» el espacio del ciberespacio: robots araña [*web spiders*], que recopilan datos para los motores de búsqueda de la web; navegadores, que buscan cosas que ver a través de la red; hackers (de los buenos) que comprueban las cerraduras de los espacios para ver si están bien cerradas; y hackers (de los malos) que las fuerzan para entrar a robar. A la ley le resulta difícil saber a priori qué agentes están usando el espacio legítimamente y cuáles no. La legitimidad depende de la intención de la persona que permite el acceso a su espacio.

Esto fue, pues, lo que llevó a Reeves a su idea: dado que la intención del «propietario» es tan crucial aquí, y dado que las vallas del ciberespacio pueden construirse de modo que reflejen dicha intención de forma barata, es mejor trasladar al propietario todos los incentivos para que sea éste quien defina el acceso a su espacio como le plazca. El derecho a navegar debería ser la norma, y la carga de cerrar las puertas debería recaer sobre el propietario.[4]

Dejemos de lado ahora la argumentación de Reeves, y pensemos por un instante en algo que parecerá completamente diferente pero que alude exactamente a la misma idea. Pensemos en el «robo» y en las protecciones que tenemos contra él:

– Si tengo una pila de leña detrás de mi casa, nadie la robaría. Si dejara mi bicicleta fuera durante toda la noche, desaparecería.

– Un amigo me contó que en una ciudad costera muy concurrida, las autoridades municipales desistieron de plantar flores porque la gente se las llevaban enseguida. Pero ahora, me informa orgullosamente mi amigo, tras una larga campaña de «espíritu comunitario», ya nadie se las lleva.

– Existen leyes especiales relativas al robo de automóviles, aviones y embarcaciones, pero no relativas al robo de rascacielos. Los coches, aviones y embarcaciones necesitan protección, mientras que los rascacielos se cuidan solos en buena medida.

---

4 Maureen O'Rourke ha extendido la idea de las vallas tecnológicas que podrían disponerse en proveer el ciberespacio, describiendo las técnicas que se podrían usar, por ejemplo, para controlar, o bloquear los sitios web, los vínculos de un sitio a otro; véase «Fencing Cyberspace: Drawing Borders in a Virtual World», *Minnesota Law Review*, núm. 82, 1998, pp. 610, 645–647. Véase, por ejemplo, *Thrifty-Tel, Inc. vs. Bezenek,* 46 Cal. App. 4Th 1559, Cal. Ct. App. 1996 (demanda de desposesión de bien mueble [*trespass to chattel claim*] relativa a la intrusión informática de los hijos del demandado para hacerse con el código confidencial del demandante con el fin de realizar llamadas telefónicas de larga distancia); *Intel vs. Hamidi,* 30 Cal. 4Th 1342, Cal. 2003 (demanda de desposesión de bienes muebles interpuesta contra Hamidi, un antiguo trabajador de Intel que usó su lista de distribución de empleados para enviarles correos electrónicos); *eBay vs. Bidder's Edge,* 100 F. Supp. 2D 1058, D. Cal. 2000 (eBay trató de impedir que Bidder's Edge, un sitio de agregación de subastas por Internet, usara una función de consulta automatizada sin la autorización de eBay); *Register.com vs. Verio,* 356 F. 3d 393, 2º Cir. 2004 (Register.com trató de impedir que Verio usara su marca registrada o sus bases de datos *online* para solicitar negocios de listas proporcionadas en el sitio web de Register.com); *America Online, Inc. vs. IMS,* 1998 U.S. Dist. LEXIS 20645, D.Va. 1998 (America Online alegó que IMS estaba enviando masivamente correos publicitarios no solicitados a sus miembros en violación de la *Lanham Act*, 15 U.S.C.S

Muchas cosas protegen las propiedades contra el robo —de forma diferente. El mercado protege mi leña (sale más barato comprarse su propia leña que llevarse la mía), pero constituye una amenaza especial para mi bicicleta (que se puede vender fácilmente si se la llevan). Unas veces las normas protegen las flores de los parques, y otras no. En ocasiones la naturaleza conspira con los ladrones (coches, aviones y embarcaciones), y en ocasiones contra ellos (rascacielos).

Estas protecciones no son fijas. Podría atar mi bicicleta con un candado y usar así el código del espacio real para dificultar que me la roben. Podría haber escasez de leña, con lo que aumentaría su demanda y sería más difícil de proteger. Puede que las campañas públicas acerca de la belleza cívica acaben con el robo de flores; también podría hacerlo la selección de una flor distintiva. Las cerraduras sofisticadas podrían inutilizar los coches robados; el fraude bancario sofisticado podría hacer vulnerables los rascacielos. Lo importante no es que las protecciones vengan dadas o sean inmodificables, sino que se multiplican y sus modalidades son diferentes.

La propiedad está protegida por la suma de las diferentes protecciones que ofrecen la ley, las normas, el mercado y el código del espacio real. Esta es la implicación del argumento expuesto en el Capítulo 7. Desde el punto de vista del Estado, sólo necesitamos la ley cuando las otras tres modalidades dejan vulnerable una propiedad. Desde el punto de vista del ciudadano, el código del espacio real (como las cerraduras) es necesario cuando las leyes y las normas por sí solas no ofrecen suficiente protección. Comprender cómo se protege la propiedad implica comprender cómo estas diferentes protecciones actúan conjuntamente.

La idea de Reeves y estas reflexiones acerca de la leña y los rascacielos indican las diferentes maneras en que la ley podría proteger la «propiedad», y sugieren los tipos de propiedad que podría intentar proteger. Asimismo, dan pie a una pregunta que ya han planteado el juez Stephen Breyer y otros muchos: ¿acaso debería la ley proteger ciertos tipos de propiedad —en concreto, la propiedad intelectual?[5]

---

5 Véase, por ejemplo, Stephen Breyer, «The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs», *Harvard Law Review*, núm. 84, 1970, p. 281.

Entre los tipos de propiedad que la ley podría proteger, en este capítulo me centraré en la propiedad protegida mediante copyright;[6] se dice que ésta es la más vulnerable a las transformaciones que traerá el ciberespacio, hasta el punto que muchos creen que es imposible proteger la propiedad intelectual allí. En los términos que he esbozado hasta ahora, podemos empezar a ver por qué se puede pensar esto, si bien pronto comprobaremos que tal pensamiento resulta erróneo.

Acerca de los informes sobre la muerte del copyright

Grosso modo, el régimen de copyright concede a su titular ciertos derechos exclusivos sobre la obra, incluyendo, por supuesto, el derecho exclusivo sobre la copia de dicha obra. Yo soy el titular del copyright de este libro, lo cual implica, entre otros derechos, y siempre respetando ciertas excepciones importantes, que el lector no lo puede copiar sin mi permiso.[7] Este derecho está protegido en la medida en que las leyes (y las normas) lo respaldan, y está amenazado en la medida en que la tecnología facilite la copia. Si se refuerza la ley al tiempo que se mantiene constante la tecnología, el Derecho queda fortalecido. Si prolifera la tecnología de copia al tiempo que se mantiene constante la ley, el Derecho queda debilitado.

---

6 Existe un debate feroz acerca de si deberíamos o no emplear el término «propiedad intelectual» para referirnos conjuntamente a estas formas separadas de regulación —copyright, patentes y marcas registradas. Yo mismo he tomado partido en uno y otro sentido en este debate, pero actualmente creo que es perjudicial no referirnos a estos distintos cuerpos legales como «propiedad intelectual». Aunque se trata, por supuesto, de ámbitos diferentes, llamarlos con el mismo nombre no necesariamente genera confusión (nadie confunde un tigre con un gatito, por más que a ambos se los llame «felinos»). Más importante aún, al no llamarlos con el mismo nombre, perdemos la oportunidad de señalar las contradicciones en que se incurre al tratar estas diferentes formas de propiedad. Por ejemplo, tanto las patentes como las marcas registradas se benefician de importantes formalidades introducidas en cada uno de esos sistemas; cuando nos percatamos de que dichas formalidades están ausentes del «copyright», podemos llegar a preguntarnos por qué una forma de «propiedad intelectual» está libre de formalidades mientras que las otras dos no lo están.

7 De manera estricta, para esta edición regida por la legislación española, Lessig sería el titular de los derechos de autor y al dotar a la obra de una licencia Creative Commons, el público tendría libre derecho de copia y distribución. [N. del E.]

En este sentido, el copyright siempre ha estado en guerra con la tecnología. Antes de la imprenta, no había mucha necesidad de proteger el interés que un autor tuviera en su obra creativa, ya que la obtención de una copia era tan cara que la propia naturaleza protegía ese interés. Pero a medida que se ha reducido el coste de la copia y aumentado la expansión de las tecnologías de impresión, la amenaza al control del autor se ha incrementado. Y como cada generación ha desarrollado una tecnología mejor que la anterior, la capacidad del titular del copyright de proteger su propiedad intelectual se ha visto debilitada.

Hasta hace poco, la respuesta que ha dado la ley a estas transformaciones era mesurada y gradual. Cuando, a comienzos del siglo XX, surgieron las tecnologías de grabación y reproducción de sonido, los compositores se sintieron amenazados. La ley respondió concediéndoles un derecho nuevo, pero limitado, a beneficiarse de las grabaciones. Cuando comenzó a emitirse música por la radio, se reconoció que los compositores tenían derecho a una compensación por la interpretación pública de su obra, pero no se compensó a los intérpretes de sus canciones por dicha «interpretación». El Congreso decidió no remediar este problema. Cuando la televisión por cable empezó a retransmitir programas televisivos, los titulares del copyright de las emisiones originales se quejaron de que se estaba explotando su trabajo sin que ellos recibieran compensación alguna. El Congreso respondió concediéndoles un derecho nuevo, pero limitado, a beneficiarse de las retransmisiones. Cuando los videos domésticos simplificaron la grabación de contenido bajo copyright emitido por televisión, los titulares del copyright clamaron contra la «piratería». El Congreso decidió no responder a esa queja. Unas veces las transformaciones tecnológicas inspiraron al Congreso a crear nuevos derechos, y otras no. Sea como fuere, a lo largo de toda esta historia, las nuevas tecnologías han sido adoptadas en la medida en que posibilitaban la difusión de la cultura.

Durante el mismo periodo, las normas relativas al contenido sujeto a copyright también evolucionaron, si bien el rasgo singular y definitorio de dichas normas quizá puede resumirse de este modo: un consumidor podía hacer lo que quisiera con el contenido bajo copyright que poseía legalmente sin que en ningún caso ello fuera competencia de la ley de derechos de autor. Esta norma era cierta casi por definición hasta 1909, ya que antes de ese año la ley no regulaba las «copias». En consecuencia, era altamente improbable que cualquier uso que hiciera un consumidor del contenido bajo copyright conculcara cualquiera de los derechos exclusivos del copyright. Después de 1909, y aunque técnicamente la ley regulaba las «copias», las tecnologías de reproducción estaban ampliamente disponibles. Se produjo una batalla legal en torno a las máquinas Xerox, la cual obligó a efectuar una pequeña

reforma,[8] pero el primer conflicto real entre la ley de copyright y los consumidores ocurrió cuando las cintas de casette facilitaron la copia de música grabada. Dichas copias estaban destinadas en parte a grabar «recopilatorios», y en parte a evitar la necesidad de comprar la cinta original. Tras muchos años de debate, el Congreso decidió no prohibir las grabaciones caseras y, en lugar de eso, señaló muy claramente en la AHRA (*Audio Home Recording Act*, Ley de Grabaciones Caseras de Audio) una serie de exenciones legales para realizar dicha actividad. Esto consolidó entre los consumidores la norma de que eran libres por ley de hacer lo que quisieran con las obras bajo copyright. Dadas las tecnologías que la mayoría de consumidores tenía a su alcance, los usos que quisieran dar a dichas obras no competían al copyright (por ejemplo, revender sus libros a una librería de segunda mano); y si lo hacían, se modificaba la ley para protegerlos (por ejemplo, con las cintas de casette).

En el marco de estos cambios graduales de la ley y de la norma práctica según la cual la ley generalmente no alcanzaba a los consumidores, las transformaciones de la tecnología digital supusieron un choque considerable. En primer lugar, desde la perspectiva tecnológica, las tecnologías digitales, a diferencia de las analógicas, permitían obtener copias perfectas de una obra original, con lo que el beneficio derivado de la copia aumentaba. En segundo lugar, y desde la misma perspectiva, la tecnología digital de Internet permitía que el contenido se distribuyera de forma libre (y anónima) a través de la red, con lo que la disponibilidad de copias aumentaba. En tercer lugar, desde la perspectiva normativa, los consumidores, que habían, interiorizado que podían hacer con «su contenido» lo que quisieran, utilizaron estas nuevas herramientas digitales para que «su contenido» estuviera ampliamente disponible en Internet. Compañías como Napster contribuyeron a impulsar esta conducta, si bien la práctica existía antes de Napster y seguiría existiendo después. En cuarto lugar, desde la perspectiva legal, poco podía hacer la ley para detener esta compartición masiva de contenido, ya que la tecnología básica de Internet no revelaba nada sobre la naturaleza del contenido distribuido en la red, ni sobre quién lo compartía. Por consiguiente, en quinto lugar, y desde la perspectiva de los titulares del copyright, las tecnologías digitales e Internet constituían una catástrofe para su modelo de negocio:

---

8 Paul Goldstein, *Copyright´s Highway: From Gutenberg to the Celestial Jukebox*, Stanford (Cal.), Stanford University Press, 2003, pp. 64, 103: «En aquella época apenas me di cuenta de que todo esto iba a tener su efecto en la televisión, en el cine, en los videos domésticos y en todo el espectro de cosas que abarca la ley de copyright, lo cual ni nos planteamos cuando adoptamos nuestra decisión. En aquel entonces lidiábamos con una operación bastante simple —la que afectaba a Xerox—, pero ahora la cuestión se ha vuelto terriblemente compleja».

si hasta entonces habían ganado dinero controlando la distribución de las «copias» de contenidos sujetos a copyright, podemos entender perfectamente por qué contemplaban Internet como una grave amenaza.

De forma muy rápida y bastante temprana, la industria de contenidos respondió a esta amenaza. Su primera línea de defensa consistió en propugnar un régimen de regulación más agresivo ya que, pese a las predicciones de los expertos en el ciberespacio, no todos estaban dispuestos a reconocer que la ley de derechos de autor estaba muerta. Los abogados especializados en propiedad intelectual y los grupos de interés presionaron desde muy pronto para que la ley apuntalara las protecciones sobre la propiedad intelectual que el ciberespacio parecía encaminado a eliminar.

La ley al rescate

La respuesta inicial a esta presión consistió en la elaboración de un Libro Blanco por el Departamento de Comercio, en 1995, en el que se esbozaban una serie de modificaciones destinadas, según sus redactores, a restaurar el «equilibrio» en la ley de propiedad intelectual. Titulado «Propiedad Intelectual y la Infraestructura Nacional de Información», este informe se afanaba por reformular la legislación existente sobre propiedad intelectual en términos que cualquiera pudiese entender, así como por recomendar modificaciones legales en respuesta a las transformaciones que la red traería consigo. Ahora bien, tal y como los eruditos señalaron rápidamente, la primera parte era un despropósito.[9] Y es que el informe «reformulaba» la legislación existente de modo semejante a la «reformulación» de los relatos

9 «Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights», U.S. Department of Commerce, 1995; en adelante, «Libro Blanco». George Smirnoff III («Copyright on the Internet: A Critique of the White Paper's Recommendation for Updating the Copyright Act and How the Courts Are Already Filling in Its Most Important Shortcoming, Online Service Provider Liability», *Cleveland State Law Review*, núm. 44, 1996, p. 197) señala vacíos importantes en el Libro Blanco, contradicciones y la aparente falta de un estudio adecuado; véase también Pamela Samuelson, «The Copyright Grab», *Wired*, enero de 1996, pp. 134-136. En contraste, Gary W. Glisson («A Practitioner's Defense of the White Paper», *Oregon Law Review*, núm. 75, 1996, p. 277) sostiene que el Libro Blanco no es ni un resumen desorientador del estado de la legislación de propiedad intelectual, ni una propuesta de cambios profundos en este ámbito. Para un amplio análisis de las cuestiones relativas al copyright que plantea el ciberespacio, véase Trotter Hardy, «Project Looking Forward: Sketching the Future of Copyright in a NetworkedWorld», informe final de la Oficina de Copyright de EEUU, 1998, disponible en http://www.copyright.gov/reports/thardy.pdf.

de los historiadores soviéticos en la época de Stalin. La reformulación se inclinaba de forma palmaria en dirección al incremento de la protección de la propiedad intelectual, pero fingía que tal inclinación se debía a la pendiente natural del terreno.

No obstante, para nuestro interés, lo más significativo del Libro Blanco son las recomendaciones que incluía. Y es que el gobierno estadounidense proponía cuatro respuestas a la amenaza que representaba el ciberespacio, las cuales nos deberían resultar familiares en los términos del Capítulo 7.

La primera respuesta era la tradicional. El gobierno proponía cambios en la ley de copyright que «clarificaran» los derechos que debía proteger.[10] Estos cambios pretendían definir mejor los derechos consagrados en la legislación de propiedad intelectual y dotarlos de un mayor respaldo mediante el establecimiento de penas legales claras (y posiblemente mayores) por su trasgresión.

La segunda respuesta se dirigía a las normas, específicamente a las concernientes a la copia. El informe recomendaba incrementar los esfuerzos educativos, tanto en las escuelas como entre el público general, en torno a la naturaleza de la propiedad intelectual y la importancia de protegerla. En los términos del Capítulo 7, estamos ante el uso de la ley para modificar las normas de modo que éstas respalden mejor la protección de la propiedad intelectual. Se trata, pues, de una regulación indirecta de la conducta por medio de la regulación directa de las normas.

Las respuestas tercera y cuarta combinaban la tecnología y el mercado. Así, el informe demandaba el respaldo legal —a través de subvenciones económicas y protección legal especial— de los «esquemas de gestión del copyright». Tales «esquemas» no eran más que tecnologías que harían más fácil controlar el acceso y el uso del material sujeto a derechos de autor. Más adelante, en este mismo capítulo, exploraremos con cierta extensión estos «esquemas», pero los menciono ahora como otro ejemplo de regulación indirecta —que usa el mercado para subvencionar el desarrollo de una cierta herramienta de software, y usa la ley para regular las propiedades de

---

10 Para un resumen de los cambios que reclamaba el Libro Blanco, véase Bruce Lehman, intervención previa al «Congreso Inagural Engelberg sobre Cultura y Economía de Participación en un Régimen de Propiedad Intelectual Internacional», reimpresión en *New York University Journal of International Law and Politics*, núm. 29, 1996–97, pp. 211, 213–215; «Libro Blanco», *op. cit.*, p. 17.

otras de esas herramientas. Los sistemas de gestión del copyright serían respaldados por la financiación gubernamental, así como por la amenaza de sanciones penales para cualquiera que implementara un software para eludirlos.[11]

El Congreso siguió las recomendaciones del Libro Blanco en ciertos aspectos, destacando en este sentido la promulgación de la DMCA (*Digital Millennium Copyright Act*, Ley de Copyright del Milenio Digital) en 1998. Ese estatuto implementó directamente la recomendación de que las «medidas de protección tecnológica» estuviesen cubiertas por la ley, de modo que el código que alguien implementaba para controlar el acceso o el uso de una obra sujeta a derechos de autor obtuvo protección legal bajo la DMCA: en consecuencia, sortear ese código, con unas pocas excepciones importantes, constituía a partir de entonces una vulneración de la ley.

Más adelante volveremos a la DMCA, pero ahora mismo la cuestión es reconocer algo importante acerca de la suposición que subyace bajo el Libro Blanco. El paquete de propuestas de 1995 era una mezcla de técnicas —algunos cambios legales, cierto respaldo a la modificación de las normas y mucho respaldo a la transformación del código del ciberespacio para mejorar su capacidad de proteger la propiedad intelectual. Quizá en 1995 no podía esperarse nada mejor que esto —la ley prometía unas respuestas moderadas para abordar el equilibrio cambiante provocado por el ciberespacio.

El equilibrio es algo atractivo y la moderación parece ser lo correcto, pero se echa en falta algo en este enfoque. El Libro Blanco procede como si el problema de proteger la propiedad intelectual en el ciberespacio fuera exactamente igual que el problema de protegerla en el espacio real. Procede como si las cuatro restricciones fueran a operar en él en las mismas proporciones que en el espacio real, como si nada fundamental hubiera cambiado.

Sin embargo, de hecho, algo fundamental ha cambiado: el papel que el código desempeña en la protección de la propiedad intelectual. El código puede desplazar a la ley, y lo hará cada vez más, como la principal defensa de la propiedad intelectual en el ciberespacio. Así pues, allí imperarán las vallas privadas, no la ley pública.

---

11 La más importante de estas amenazas es la disposición legal relativa a la anti-elusión de la DMCA, la cual establece como delito (sujeto a complejas excepciones) la fabricación de código destinado a eludir un mecanismo de protección del copyright, incluso aunque el propio uso del material subyacente se considere «uso justo» [*fair use*]; véase Pub.L. 105–304, 112 Stat 2877, 1998 (que prohíbe la fabricación, importación o distribución de «dispositivos, productos, componentes» que «frustren los métodos tecnológicos que impiden el uso no autorizado»).

El Libro Blanco no captó esto. Entre el popurrí de ideas que contiene, se incluye una crucial para su enfoque, pero que es fundamentalmente incorrecta —la idea de que la naturaleza del ciberespacio es el caos. El Libro Blanco promete reforzar la ley en todas las áreas donde sea posible, pero se aproxima a la cuestión como un barco que asegura las escotillas ante una tormenta: pase lo que pase, la amenaza al copyright es real y causará daños, y lo mejor que se puede hacer es capear el temporal.

Esta idea es fundamentalmente errónea. Y es que no estamos entrando en una era en que el copyright esté más amenazado que en el espacio real, sino más bien en una era en la que está protegido de forma más efectiva que nunca desde los tiempos de Gutenberg. El poder de regular el acceso y el uso del material sujeto a derechos de autor está a punto de ser perfeccionado. Independientemente de lo que pudieran pensar los eruditos de mediados de la década de los noventa, el ciberespacio está a punto de otorgarles a los titulares de derechos de autor la mayor protección que jamás hayan conocido.

En una era como ésta, la verdadera pregunta que ha de plantearse la ley no es cómo puede contribuir a esta protección, sino más bien si ésta es demasiado amplia. Los eruditos mencionados tenían razón cuando predijeron que el ciberespacio nos enseñaría que todo lo que sabíamos hasta el momento sobre derechos de autor estaba equivocado.[12] Ahora bien, la lección que nos ofrecerá el futuro será, que el copyright está protegido de manera excesiva. El problema se centrará entonces, no en el derecho de copia sino en el *deber* de copia —el deber que tienen los propietarios de obras protegidas de hacerlas accesibles.

Ésta es una afirmación de gran trascendencia. No obstante, para captar su sentido y las consecuencias que comporta necesitamos considerar tres ejemplos. El primero se refiere a la visión de un investigador del centro de investigación Xerox PARC (que viene muy al caso), Mark Stefik, y su idea de los «sistemas de confianza».[13]

---

12 Véase John Perry Barlow, «The Economy of Ideas», *Wired*, marzo de 1994, p. 129; véase también John Perry Barlow, «Papers and Comments of a Symposium on Fundamental Rights on the Information Superhighway», *Annual Survey of American Law*, 1994, pp. 355, 358. Barlow sostiene que «no es tan fácil poseer aquello que jamás ha tenido dimensión física alguna», a diferencia de las formas tradicionales de propiedad. «Hemos tendido a pensar», añade, «que el copyright funcionaba bien porque era difícil transportar físicamente las propiedades del intelecto sin antes expresarlas en algún soporte físico; y eso ya no es necesario».

13 Véase Mark Stefik, «Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing», *Berkeley Technology Law Journal*, núm. 12, 1997, p. 137; Mark Stefik, «Trusted Systems», *Scientific American*, marzo de 1997, p. 78; Mark Stefik, «Letting Loose the Light: Igniting Commerce in Electronic Publication», en Stefik (ed.), *Internet Dreams*, *op. cit.*, pp. 220–222, 226–228.

El segundo alude a una de las implicaciones de un mundo dominado por los sistemas de confianza. El tercero apunta a un coste no computado en la senda que hemos tomado para «proteger la propiedad intelectual». Tales ejemplos pondrán de relieve la amenaza que dichos cambios representan para una serie de principios que nuestra tradición considera fundamentales. Asimismo, los ejemplos deberían obligarnos a tomar una decisión acerca de dichos principios y del lugar que ocuparán en nuestro futuro.

La promesa para la propiedad intelectual en el ciberespacio

> Todo depende de si entiendes en profundidad la idea de los sistemas de confianza. Si no la entiendes, todo este enfoque del comercio y la edición digital resulta completamente inconcebible; si la entiendes, entonces, todo lo demás encaja.
>
> Ralph Merkle, citado en Stefik, *Letting Loose the Light*, 1996.

En el contexto de lo que denominamos la primera generación de las tecnologías digitales, los propietarios de los contenidos eran incapaces de controlar quién copiaba qué. Si el lector posee una copia de una fotografía sujeta a copyright en un archivo gráfico, podría copiarla ilimitadamente sin que ello produzca ningún efecto sobre el original. Cuando el lector realiza la centésima copia del archivo, nada indica que es la centésima y no la primera. Y como hemos descrito una y otra vez, no había nada en el código original de Internet que regulara cómo y a quién se distribuía el contenido bajo copyright. La función «copiar», tal y como fue desarrollada por los escritores de código que la construyeron, ya fuera en los ordenadores o en las redes informáticas, estaba destinada a «copiar» —no a «copiar» con una serie de permisos especificados.

Esta característica de la función «copiar» no era exclusiva del ciberespacio. Hemos visto una tecnología que planteaba el mismo problema, y ya he descrito cómo se introdujo posteriormente una solución.[14] La tecnología DAT fue considerada en su momento una amenaza para los titulares de

14 Véase Joel R. Reidenberg, «Governing Networks and Rule-Making in Cyberspace», *Emory Law Journal*, núm. 45, 1996, p. 911.

derechos de autor, ante la cual se propusieron distintas remedios: algunos abogaron por un incremento de las penas por la copia ilegal de cintas (regulación directa mediante la ley); otros, como Richard Stallman, defendieron un impuesto sobre las cintas vírgenes que compensara a los titulares del copyright (regulación indirecta del mercado por parte de la ley); otros reivindicaron una mejor educación para acabar con la copia ilegal de cintas (regulación indirecta de las normas por parte de la ley); pero hubo también quien sostuvo que había que modificar el código de las DAT para así bloquear la copia ilimitada y perfecta.

Finalmente salieron adelante las soluciones basadas en la introducción del impuesto y de la regulación del código. A finales de 1992 el Congreso promulgó la AHRA como un acuerdo entre la tecnología y las industrias de contenidos. Esta ley introdujo de entrada un impuesto tanto sobre las cintas vírgenes como sobre los grabadores, destinando los ingresos a compensar a los titulares de derechos de autor por la infracción de copyright que se preveía que favorecería la tecnología digital. Más interesante resulta, sin embargo, que la ley exigiera a los fabricantes de tecnología DAT la inclusión de un «sistema de gestión de copias en serie» que limitara la capacidad de copia de dicha tecnología. Tal límite se introdujo a través de un código inserto en las copias efectuadas mediante tecnología DAT. Con él siempre se podía realizar una copia digital a partir del original, pero no a partir de una copia hecha en un grabador DAT. (A partir de esta, podía realizarse una copia analógica, con la consiguiente merma de calidad, pero no otra copia digital perfecta). Así pues, la tecnología se diseñó para inhabilitar la función «copiar» bajo determinadas condiciones, de modo que se protegiera indirectamente a los propietarios del copyright. El efecto neto de estos dos cambios fue minimizar cualquier perjuicio derivado de la tecnología, así como limitar la funcionalidad de la tecnología allí donde se esperaba que ésta propiciara la violación del copyright. (Muchos estiman que el efecto neto de esta regulación también mató la tecnología DAT).

Una idea similar animó la visión de Stefik,[15] si bien él no era partidario de reducir la calidad de las copias. En lugar de esto, su objetivo era posibilitar el seguimiento y control de las copias de contenido digital que se llevaran a cabo.[16]

---

15 Véase Mark Stefik, «Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing», *Berkeley Technology Law Journal*, núm. 12, 1997.

16 En «Shifting the Possible», *op. cit.*, pp. 142–144, Stefik plantea cómo las impresoras de confianza combinan cuatro elementos —derechos de impresión, distribución *online* cifrada, facturación automática por las copias y marcas de agua digitales— con el fin de vigilar y controlar las copias que efectúan.

Reflexionemos sobre esta propuesta del siguiente modo. Hoy, cuando el lector compra un libro, puede hacer una serie de cosas: puede leerlo una vez o cien veces; puede prestárselo a un amigo; puede fotocopiar algunas páginas o escanearlo en su ordenador; puede quemarlo, usarlo como pisapapeles o venderlo; puede colocarlo en la estantería de su casa y jamás llegar a abrirlo.

El lector puede hacer algunas de estas cosas porque la ley reconoce su derecho a hacerlas —por ejemplo, el lector puede vender el libro porque la legislación de derechos de autor limita explícitamente el derecho del propietario del copyright a controlar el uso que el lector haga del libro físico después de la «primera venta». Otras cosas las puede hacer porque no existe un modo efectivo de impedírselo. Un librero podría venderle el libro al lector a un precio si este promete leerlo una sola vez, y a otro precio si desea leerlo cien veces, pero aquél no tiene modo de averiguar si éste ha obedecido el contrato. En principio, el librero podría vender con cada libro un agente de policía para seguir la pista al lector y asegurarse de que usa el libro tal y como prometió, pero los costes de este control excederían claramente cualquier posible beneficio.

Ahora bien, ¿qué sucedería si cada uno de estos derechos pudiera controlarse y ser disgregado y vendido por separado? ¿Qué sucedería si el propio software pudiera regular si leemos el libro una o cien veces; si podemos copiar y pegar fragmentos de él o simplemente leerlo sin copiarlo; si podemos enviarlo adjunto a un amigo o simplemente conservarlo en nuestro ordenador; si podemos borrarlo o no; si podemos usarlo para otra obra, con cualquier fin, o no; o si podemos simplemente dejarlo en la estantería o también tenerlo y usarlo?

Stefik describe una red que hace posible esta disgregación de derechos, una arquitectura que permitiría a los propietarios de material bajo copyright vender el acceso en los términos que deseen y que garantizaría el cumplimiento de estos contratos.

Los detalles de este sistema no son importantes aquí (se basa en la arquitectura de cifrado que describí en el Capítulo 4),[17] si bien su concepción general resulta bastante fácil de describir. Según el diseño actual de la red, las funciones básicas de copia y acceso están reguladas crudamente según el principio de «todo o nada». Por regla general, se tiene derecho a copiar o no se tiene, se tiene derecho a acceder o no se tiene.

17 *Ibidem*.

No obstante, podría incluirse un sistema de derechos más sofisticado en la Red —no en una red diferente, sino sobre la Red actual. Este sistema funcionaría mediante la discriminación en las relaciones que establezca con otros sistemas. Un sistema que controlara el acceso de este modo más sutil sólo permitiría acceder a sus recursos a otro sistema que controlara el acceso del mismo modo. De esta manera, se desarrollaría una jerarquía de sistemas y sólo se intercambiaría material sujeto a copyright entre aquellos sistemas que controlaran adecuadamente el acceso.

En un mundo semejante, pues, podríamos acceder, por ejemplo, al *New York Times* y pagar un precio diferente en función de cuánto leamos. El periódico podría determinar cuánto leemos, si podemos copiar partes del diario, si podemos archivar noticias en nuestro disco duro, etc. Ahora bien, si el código que usamos para acceder al sitio del *New York Times* no permitiera el control que exige el periódico, entonces éste nos vetaría el acceso. En pocas palabras, los sistemas intercambiarían información sólo con aquellos otros sistemas en los que pudieran confiar, y los protocolos de confianza se incluirían en las arquitecturas de los sistemas.

Stefik denomina a esto los «sistemas de confianza», nombre que evoca una analogía muy útil. Pensemos en los mensajeros asegurados. En ocasiones queremos enviar una carta que contiene algo especialmente valioso. Para ello podríamos recurrir simplemente al servicio estatal de correos, pero éste no es un sistema del todo fiable en estos casos; su control sobre sus empleados es relativamente escaso, por lo que los robos y pérdidas no son nada fuera de lo común. Así pues, en vez de ir a la oficina de correos, podríamos enviar la carta por medio de un mensajero asegurado, cuyo seguro representa un coste que le obliga a ser fiable. Esta reputación posibilita que quien envíe material valioso cuente con una garantía del servicio que contrata. Como escribe Stefik:

> con los sistemas de confianza, una parte sustancial de la aplicación de un contrato digital es efectuada por el propio sistema. El consumidor no tiene la opción de incumplir un contrato digital a través de, por ejemplo, la realización de copias no autorizadas de una obra. Un sistema de confianza se niega a ejercer todo derecho que no esté sancionado por medio de un contrato digital.[18]

Esto es lo que una estructura de sistemas de confianza hace por los propietarios de derechos de autor. Es como un mensajero asegurado que recibe el objeto de valor y controla cómo se accede a él y si se usa de acuerdo con las órdenes que le da la dirección.

---

18 Stefik, *The Internet Edge*, *op. cit.*, p. 91.

Imaginémonos por un instante que una estructura así se implantara de forma general en el ciberespacio. ¿Cómo pensaríamos entonces acerca de la legislación de copyright?

Un aspecto importante de dicha legislación es que, por más que se diseñara en parte para proteger a los autores, no contemplaba que estos ejercieran un control perfecto sobre su obra. Como señaló el Tribunal Supremo, esta «protección nunca ha concedido al propietario del copyright un control completo sobre todos los posibles usos de su obra».[19] En consecuencia, la ley sólo otorga ciertos derechos exclusivos, y éstos están sujetos a importantes limitaciones, como el uso justo [*fair use*], la limitación temporal y la doctrina de la primera venta. Por lo tanto, la ley amenazaba con castigar a quienes violasen el copyright —y esta amenaza fue la que hizo que un importante porcentaje de la población se sometiera a ella—, pero nunca fue concebida meramente para cumplir la voluntad de los autores. Los intereses de éstos debían conjugarse, pues, con una finalidad genuinamente pública.

Los sistemas de confianza proporcionan a los autores el mismo tipo de protección. Como éstos pueden restringir el uso no autorizado de su material, pueden obtener dinero a cambio del acceso. De esta manera, los sistemas de confianza logran lo que la ley se propone, pero sin necesidad de contar con las restricciones legales para respaldar su protección. Así pues, estos sistemas permiten un control mucho más sutil sobre el acceso y el uso de material protegido que el que posibilita la ley, pero pueden hacerlo sin la ayuda de ésta.

Lo que el copyright trata de hacer mediante la amenaza de la ley y la presión de las normas, los sistemas de confianza lo ejecutan a través del código. El copyright ordena que se respeten los derechos del titular de derechos de autor antes de usar su propiedad; los sistemas de confianza sólo permiten acceder a ésta si antes se han respetado los derechos correspondientes. Los controles necesarios para regular este acceso se incluyen dentro de los sistemas, y ningún usuario (que no sea un hacker) tiene opción de desobedecerlos. De esta manera, el código complementa la ley codificando las reglas, haciéndolas más eficaces.

En este sentido, los sistemas de confianza constituyen una alternativa privatizada a la legislación de derechos de autor. Dichos sistemas no han de ser los únicos; no hay razón para no usarlos en combinación con la ley.

---

19 *Sony vs. Universal Studios, Inc.*, 464 U.S. 417, 432, 1984.

Sea como fuere, lo cierto es que el código está asumiendo *de facto* una tarea que corresponde a aquélla, pues implementa la protección legal, por medio del código, de un modo mucho más efectivo de lo que lo hacía la ley.

¿Qué podría haber de malo en esto? Nadie se preocupa cuando la gente instala cerrojos dobles en sus puertas para complementar la labor de la policía de barrio, ni cuando cierra su coche y se guarda la llave. No hay nada ofensivo en protegerse uno mismo en lugar de confiar esa tarea al Estado. De hecho, en ciertos contextos, constituye una virtud. Así, por ejemplo, la madre de Andrew Jackson, séptimo presidente de EEUU, le aconsejó cuando partía a luchar en la Guerra de Independencia: «Nunca digas mentiras, ni tomes lo que no te pertenece, ni demandes a nadie por difamación o lesiones. Todos estos problemas, arréglalos por ti mismo».[20] En casos como éstos, la autosuficiencia es un signo de fortaleza y el recurso a la ley, de debilidad.

Hemos de dar dos pasos para responder a la pregunta formulada en el párrafo anterior. El primero recupera una idea acerca de la naturaleza de la «propiedad» que, pese a resultarnos familiar, solemos olvidar; el segundo expone una noción menos familiar, pero esencial, acerca de la naturaleza de la propiedad intelectual. Considerados en su conjunto, estos pasos apuntan a la razón por la que el control perfecto no es el control que la ley ha concedido a los titulares de la propiedad intelectual, así como al problema potencial que creará la legislación de copyright en el ciberespacio.

Los límites de la protección de la propiedad

En la historia legal de EEUU, los realistas (entre 1890 y 1930, aproximadamente) eran eruditos que (en parte) enfatizaron el papel del Estado en lo que se denominaba la «ley privada».[21] En la época en la que expusieron sus

---

20 Véase David Hackett Fischer, *Albion's Seed: Four British Folkways in America*, Nueva York, Oxford University Press, 1989, p. 765.

21 Véase William W. Fisher III *et al*. (eds.), *American Legal Realism*, Nueva York, Oxford University Press, 1993, pp. 98–129; John Henry Schlegel, *American Legal Realism and Empirical Social Science*, Chapel Hill, University of North Carolina Press, 1995. Para un buen ejemplo moderno del mismo análisis, véase Keith Aoki, «(Intellectual) Property and Sovereignty: Notes Toward a Cultural Geography of Authorship», *Stanford Law Review*, núm. 48, 1996, p. 1293.

análisis, era la noción de «privada» la que prevalecía en la expresión «ley privada», relegando al olvido la «ley» como si la «propiedad» y el «contrato» existieran independientemente del Estado.

El propósito de los realistas era refutar esta visión. Las leyes relativas a los contratos y la propiedad, sostenían, dota de poder a las partes privadas.[22] Si el lector incumple un contrato que ha firmado conmigo, puedo conseguir que un tribunal ordene al *sheriff* que le obligue a pagarme; el contrato me da acceso al poder estatal del *sheriff*. Si firmamos un contrato donde pone que la empresa puede despedirnos por llegar tarde, ésta puede llamar a la policía para que nos eche si nos negamos a marcharnos por nuestro propio pie. Si nuestro contrato de alquiler prohíbe tener gatos, el casero puede recurrir al poder de los tribunales para desahuciarnos en caso de que no nos deshagamos de ellos. Todos estos ejemplos muestran cómo el contrato y la propiedad, por más que se basen en la acción privada, dotan a una persona privada del respaldo del Estado.

No cabe duda de que este poder está justificado en muchos casos; llamarlo «ley» no equivale a calificarlo de injusto. La mayor prosperidad de la historia ha sido creada por un sistema en que las partes privadas podían organizar sus vidas libremente mediante los contratos y la propiedad. Ahora bien, independientemente de que tal poder estuviera o no justificado, los realistas defendían que los contornos de esta «ley» deberían diseñarse con el fin de beneficiar a la sociedad.[23]

No se trata de comunismo. No se trata de un ataque a la propiedad privada, ni supone afirmar que el Estado genera riqueza (aleje de mí el lector sus libros de Ayn Rand). Simplemente estamos ante afirmaciones acerca de la relación entre la ley privada y la ley pública que deberían estar al margen de cualquier controversia.

La ley privada crea derechos privados en la medida en que éstos sirvan al bien colectivo. Si un derecho privado atenta contra un bien colectivo, el Estado carece de motivos para crearlo, ya que los intereses estatales son generales, no particulares. El motivo que tiene el Estado para crear derechos es que éstos sirven a un propósito común, nunca particular.

---

22 Véase Fried, *The Progressive Assault on Laissez-Faire*, *op. cit.*, pp. 1–28; véase también Joel P. Trachtman, «The International Economic Law Revolution», *University of Pennsylvania Journal of International Economic Law*, núm. 17, 1996, pp. 33-34, donde señala que muchos realistas y teóricos críticos del derecho han afirmado que la expresión «ley privada» constituye un oxímoron.

23 Los jueces también han sostenido este argumento; véase *Lochner vs. New York,* 198 US 45, 74, 1905 (voto particular del juez Oliver Wendell Holmes Jr.).

La institución de la propiedad privada representa una aplicación de este argumento. El Estado posee un interés en definir derechos relativos a la propiedad privada porque ésta contribuye a producir una prosperidad general y amplia, constituyendo un sistema de ordenación de las relaciones económicas que beneficia a todos los miembros de la sociedad. Ningún otro sistema que hayamos concebido hasta el momento ordena mejor las relaciones económicas, y hay quien piensa que ningún otro podría llegar a hacerlo.[24]

Pero los derechos de propiedad nunca son absolutos, ni siquiera con la propiedad ordinaria —nuestro coche o nuestra casa. No existe ninguna propiedad que no tenga que ceder en algún momento a los intereses del Estado. El Estado puede expropiar nuestro terreno para construir una autopista, la policía puede incautar nuestro coche para llevar al hospital a la víctima de un accidente, el cartero puede atravesar el camino de entrada de nuestra casa, los inspectores de sanidad pueden inspeccionar nuestra vivienda. El sistema de propiedad que llamamos «propiedad privada» mantiene de innumerables maneras el equilibrio entre el control exclusivo del individuo y ciertos fines comunes del Estado. Cuando los segundos entran en conflicto con el primero, es éste el que ha de ceder.

Según los realistas, este equilibrio constituye un rasgo de toda propiedad, pero especialmente de la propiedad intelectual. En consecuencia, el equilibrio de derechos que rige la propiedad intelectual difiere del que rige la propiedad ordinaria de carácter personal o inmobiliario. En palabras de Boyle, «la información es diferente».[25] Un rasgo muy obvio de la propiedad intelectual nos mostrará por qué.

Cuando la ley de propiedad me concede el derecho exclusivo de usar mi casa, posee una buena razón para actuar así. Si el lector usara mi casa al mismo tiempo que yo, yo dispondría de menos espacio que usar. Y también tiene sentido que la ley me conceda un derecho exclusivo sobre mi manzana, ya que si el lector se come mi manzana, yo no me la podré comer. El uso de mi propiedad por parte de otra persona normalmente interfiere con el uso que yo hago de ella, es decir, su consumo reduce el mío.

---

24 He aquí la limitación epistemológica que se señala en la mayor parte de la obra de Friedrich A. von Hayek; véase, por ejemplo, *Law, Legislation, and Liberty*, vol. 2, Chicago, University of Chicago Press, 1978 [ed. cast.: *Derecho, legislación y libertad*, trad. por Luis Reig Albiol, Madrid, Unión Editorial, 1979].

25 Boyle, *Shamans, Software, and Spleens*, *op. cit.*, p. 174.

La ley posee, por lo tanto, una buena razón para concederme un derecho exclusivo sobre mi propiedad personal e inmobiliaria. Si no lo hiciera, yo tendría pocas razones para trabajar para producirla. O si lo hiciera, tendría que dedicar gran parte de mi tiempo a tratar de mantener alejados a los intrusos. Por lo tanto, prosigue la argumentación, es mejor para todos que yo posea un derecho exclusivo sobre mi propiedad (adquirida legalmente), puesto que así tendré un incentivo para producirla y no perderé todo mi tiempo defendiéndola de los demás.[26]

Las cosas son muy diferentes con respecto a la propiedad intelectual. Si el lector «toma» mi idea, yo sigo teniéndola. Si yo le cuento una idea, el lector no me priva de ella.[27] Un rasgo insoslayable de la propiedad intelectual es que su consumo es «no rival», tal y como gustan de calificarlo los economistas. El consumo de otro no disminuye el mío. Si escribo una canción, el lector puede cantarla sin que ello imposibilite que yo también lo haga. Si escribo un libro, el lector puede leer un ejemplar (hágalo, por favor) sin que ello impida que yo lea otro. Las ideas, en su núcleo, pueden compartirse sin que se reduzca la cantidad que su «propietario» puede consumir. Esta diferencia es fundamental, y fue comprendida ya desde la fundación de EEUU.

No en vano, Thomas Jefferson la expresó mejor que yo:

> Si la naturaleza ha creado alguna cosa menos susceptible que todas las demás de ser objeto de propiedad exclusiva, ésa es la acción del poder del pensamiento que llamamos idea, la cual sólo puede poseer un individuo si la guarda para sí; pero en el momento en que se divulga, se fuerza a sí misma a estar en posesión de todos, y su receptor no puede desposeerse de ella. Además, su peculiar carácter es tal que nadie posee menos de ella porque otros la posean íntegramente. Aquél que recibe una idea de mí, recibe instrucción para sí sin reducir la mía, del mismo modo que aquél que enciende su cirio con el mío, recibe luz sin dejarme a oscuras. El hecho de que las ideas puedan difundirse libremente de unos a otros por todo el globo, para moral y mutua instrucción de las personas y mejora de su condición, parece haber sido diseñado de forma peculiar y benevolente por la naturaleza, cuando las hizo como el fuego, susceptibles de expandirse por todo el espacio sin que disminuya su

---

26 En este relato utilitario simplificado, estoy ocultando una gran cantidad de elementos filosóficos, pero para una contundente fundamentación económica de este argumento, véase Harold Demsetz, «Toward a Theory of Property Rights», *American Economics Review*, núm. 57, 1967, p. 347.

27 Para una introducción maravillosamente clara a esta idea, así como para un completo análisis de la legislación de propiedad intelectual, véase Robert P. Merges *et al*., *Intellectual Property in the New Technological Age*, Nueva York, Aspen Law and Business, 1997, cap. 1.

> densidad en ningún punto, y como el aire que respiramos, en que nos movemos y tenemos nuestro ser físico, incapaces de ser confinadas o poseídas de forma exclusiva. Así pues, las invenciones no pueden, por naturaleza, estar sujetas a propiedad.[28]

Técnicamente, Jefferson presenta aquí dos conceptos: uno es la posibilidad de excluir a otros de usar o acceder a una idea, que define como una «acción del poder del pensamiento [...] la cual sólo puede poseer un individuo si la guarda para sí». A la pregunta de si las ideas son «exclusivas», Jefferson responde que una idea es «exclusiva» hasta «el momento en que se divulga».

El otro concepto se refiere a si mi uso de la idea divulgada disminuye el uso que otros hagan de ella. Esto plantea si las ideas divulgadas son «rivales»,[29] y Jefferson responde de nuevo que, una vez divulgadas, las ideas no son «rivales». En conclusión, Jefferson cree que el acto de divulgarlas o compartirlas hace que las ideas sean tanto «no exclusivas» como «no rivales», y que las personas podemos hacer bien poco para modificar este hecho.[30]

De hecho, las ideas que se comparten son no exclusivas y no rivales. Puedo excluir a la gente de mis ideas o escritos secretos —puedo mantenerlos en secreto o construir vallas para que no accedan. La facilidad y la efectividad de estas medidas constituyen una cuestión técnica que depende de la arquitectura de protección que proporcione un contexto dado. Pero dada la tecnología adecuada, no cabe duda de que puedo excluir a la gente de mis ideas o escritos. Lo que no puedo hacer es excluirla de ellos una vez los he compartido, simplemente, porque ya han dejado de ser mis secretos.

Las ideas que comparto también son «no rivales». Ninguna tecnología (de la que tengamos noticia) puede borrar una idea de la cabeza de una persona cuando la comparte con otra. El hecho de que yo sepa lo que sabe el

---

28 Thomas Jefferson, carta a Isaac Mcpherson, 13 de agosto de 1813, reimpresa en H. A. Washington (ed.), *Writings of Thomas Jefferson, 1790–1826*, vol. 6, Washington DC, Taylor & Matjry, 1854, pp. 180–181, citado en *Graham vs. John Deere Company*, 383 US 1, 8–9 y núm. 2, 1966.

29 Para el debate clásico, véase Kenneth J. Arrow, «Economic Welfare and the Allocation of Resources for Invention», en *The Rate and Direction of Inventive Activity: Economic and Social Factors*, Princeton (NJ), Princeton University Press, 1962, pp. 609, 616–617.

30 Para una problematización muy contundente de la perspectiva económica en este contexto, véase Boyle, «Intellectual Property Policy Online», *Harvard Journal of Law and Technology*, vol. 10, núm. 47, 1996, pp. 35–46. La obra de Boyle evidencia la indeterminación que la economía debe manifestar sobre si el incremento de derechos de propiedad sobre la información incrementaría a su vez la producción de ésta.

lector no disminuye su conocimiento al respecto. Este hecho viene dado como tal en el mundo, y determina que la propiedad intelectual sea diferente. A diferencia de lo que sucede al compartir las manzanas y las casas, puedo tomar una idea del lector sin que a éste le quede menos de ella.

No obstante, de aquí no se desprende que los derechos de propiedad sobre las expresiones e invenciones no sean necesarios.[31] Tan sólo porque el lector pueda tener lo que yo tengo sin disminuir mi propiedad no ha de concluirse que el Estado no tenga razones para crear derechos sobre las ideas o sobre la expresión de las mismas.

Si una novelista no puede impedir que copiemos su novela (en lugar de comprarla), entonces es posible que le queden escasos incentivos para escribir más obras. Puede que siga teniendo lo mismo que tenía antes de que copiásemos su libro, pero si no le pagamos por él, no tendrá incentivo económico alguno para seguir produciendo.

Qué duda cabe de que los incentivos que posee un autor resultan bastante complejos, y de que es imposible realizar generalizaciones simples al respecto.[32] Ahora bien, las generalizaciones no tienen que ser perfectas para exponer un argumento: por más que algunos autores escriben por amor al arte, sigue siendo necesario que la ley contemple algunos derechos de propiedad intelectual. Si no lo hiciera, existirían menos autores, con lo que la ley posee una razón para proteger sus derechos, al menos en cuanto que, haciéndolo, les proporciona un incentivo para producir. En el caso de la propiedad ordinaria, la ley debe crear un incentivo para producir y, al mismo tiempo, proteger el derecho de propiedad; en el de la propiedad intelectual, la ley sólo necesita crear el incentivo para producir.

He aquí la diferencia entre estos dos tipos de propiedad tan distintos, diferencia que afecta en sus fundamentos a la naturaleza de la legislación de propiedad intelectual. Así, mientras que protegemos la propiedad personal e inmobiliaria para proteger al propietario de perjuicios y proporcionarle un incentivo, protegemos la propiedad intelectual para asegurarnos de que creamos un incentivo suficiente para producirla. No obstante, este «incentivo suficiente» es algo menos que el «control

31 Algunos insisten en denominar a esto «propiedad»; véase Frank H. Easterbrook, «Intellectual Property Is Still Property», *Harvard Journal of Law and Public Policy*, núm. 13, 1990, p. 108.

32 Este es el mensaje que está presente en las obras del juez Stephen Breyer sobre copyright, por ejemplo, «The Uneasy Case for Copyright», *op. cit.*

perfecto» mencionado, con lo que, a su vez, podemos afirmar que las protecciones ideales de la ley de copyright son menores que las protecciones ideales de la propiedad ordinaria o inmobiliaria.

Esta diferencia entre la naturaleza de la propiedad intelectual y la de la ordinaria aparece reconocida en la Constitución de EEUU, que, en su artículo I, sección 8, cláusula 8, concede al Congreso el poder de «promover el progreso de la ciencia y de las artes aplicadas garantizando durante un tiempo limitado a autores e inventores el derecho exclusivo sobre sus respectivos escritos y descubrimientos».

Démonos cuenta de la estructura especial de esta cláusula. En primer lugar, establece la razón precisa del poder concedido —promover el progreso de la ciencia y de las artes aplicadas. Es por estas razones, y sólo por ellas, que el Congreso puede otorgar un derecho exclusivo. Y, en segundo lugar, fijémonos en la temporalidad especial de este derecho: «durante un tiempo limitado». La Constitución no permite que el Congreso otorgue a los autores e inventores derechos exclusivos de carácter permanente sobre sus escritos e inventos, sino sólo derechos limitados temporalmente (por más que, aparentemente, esos límites puedan ser extendidos).[33] Es decir, la Constitución no le da al Congreso el poder de conceder una «propiedad» perpetua sobre dichas obras, sino sólo un derecho exclusivo por un tiempo limitado.

Por consiguiente, la protección constitucional de la propiedad intelectual es, en sus fundamentos, diferente de la protección de la propiedad ordinaria. He afirmado antes que toda propiedad se concede sometida a las limitaciones que impone el bien público, pero incluso así, si el Estado decidiera nacionalizar todas las propiedades quince años después de haber sido adquiridas, la Constitución exigiría compensar a los propietarios. En contraste, si el Congreso fija en quince años la vigencia del copyright, no tendría que compensar a los titulares de esos derechos una vez que expirara ese plazo. Y es que los derechos de propiedad intelectual constituyen un monopolio que el Estado concede a los productores de propiedad intelectual a cambio de su producción. Una vez transcurrido un tiempo limitado, el producto de su trabajo pasa a ser de dominio público, de modo que cualquiera puede utilizarlo como desee. Estamos hablando de comunismo en el núcleo de la protección de propiedad intelectual de la Constitución estadounidense. Esta «propiedad» no constituye propiedad en el sentido habitual del término.

33 Véase *Eldred vs. Ashcroft*, 537 U.S. 186, 2003.

Y esto es cierto, asimismo, por razones mejores que las arraigadas en la tradición. Los economistas comprendieron hace mucho tiempo que otorgar derechos de propiedad sobre la información resulta peligroso (por no decir algo peor).[34] Esto no se debe a que tengan inclinaciones izquierdistas, sino a que son pragmáticos y, por lo tanto, si otorgan un derecho de propiedad es con el objetivo de facilitar la producción. Ahora bien, en principio no hay modo de saber si el aumento o disminución de los derechos concedidos por la legislación de propiedad intelectual conducirá a un incremento de dicha propiedad intelectual. Las razones de esto son complejas, pero la idea que se extrae de ahí no lo es: no hay garantía alguna de que aumentar la protección de la propiedad intelectual contribuya a «promover el progreso de la ciencia y de las artes aplicadas» —es más, a menudo no hace sino obstaculizarlo.

Tradicionalmente, la legislación de propiedad intelectual establece un equilibrio entre las protecciones que concede al autor y el uso y acceso públicos que concede al resto de personas. Su objetivo es proporcionar al autor el incentivo suficiente para producir, si bien en ella se incluyen disposiciones que limitan el poder de éste para controlar el uso de las ideas que ha creado.[35]

Un ejemplo clásico de estos límites y de esta dimensión de uso público contenida en la ley es el derecho de «uso justo» [*fair use*], que permite usar el material sujeto a copyright independientemente de los deseos de su propietario. De esta forma, si el copyright concede ciertos derechos al propietario, el uso justo entraña una limitación de dichos derechos, que permite,

---

34 Para un análisis extenso y equilibrado, véase William M. Landes y Richard A. Posner, «An Economic Analysis of Copyright Law», *Journal of Legal Studies*, núm. 18, 1989, pp. 325, 325–27, 344–46. Estos autores apuntan que, dado que las ideas son un bien público —esto es, algo que pueden usar infinidad de personas sin que se agote—, otra gente puede apropiarse fácilmente de las ideas de un creador. Por ello, la protección del copyright trata de equilibrar eficazmente los beneficios derivados de crear nuevas obras con las pérdidas que supone limitar el acceso y con los costes de administrar la protección de los derechos de autor; de este modo, dicha protección trata de promover el beneficio público que supone el avance del conocimiento y del aprendizaje por medio de un incentivo. A los autores se les ofrecen, así, las recompensas económicas del mercado con el fin de incitarlos a producir y diseminar nuevas obras (p. 326). Véase también Richard Posner, *Law and Literature*, Cambridge (Mass.), Harvard University Press, 1998, pp. 389–405 [ed. cast.: *Ley y literatura*, trad. por Pilar Salamanca, Valladolid, Cuatro y el Gato 2004]; William M. Landes y Richard Posner, *The Economic Structure of Intellectual Property Law*, Cambridge (Mass.), Harvard University Press, 2003, pp. 8–9 [ed. cast.: *La estructura económica del derecho de propiedad intelectual e industrial,* trad. por Víctor Manuel Sánchez Álvarez, Madrid, Fundación Cultural del Notariado, 2006].

35 Estos límites provienen tanto de los límites en la cláusula del copyright, que establece sus propósitos de forma muy clara, como de la Primera Enmienda; véase, por ejemplo, *Feist Publications, Inc. vs. Rural Telephone Service Co.*, 499 US 340, 346, 1991.

por ejemplo, que el lector escriba una crítica de este libro, o que seleccione partes y las reproduzca en un artículo destinado a rebatirme. De estas y otras maneras, el lector tiene el derecho de usar mi libro independientemente de cómo yo diga que se debería usar.

El uso justo, además, no necesariamente perjudica los intereses del autor —o, expresado con mayor precisión, no necesariamente perjudica a los autores como *clase*. Cuando el uso justo protege el derecho de los críticos literarios a escribir acerca de los libros sin permiso de sus autores, posibilita que surjan más críticos que elaboren más críticas. Y cuantas más críticas se escriban, mejor será la información de que disponga la gente a la hora de comprar libros y, en consecuencia, más libros se venderán. Los autores en su conjunto se benefician del sistema de uso justo, por más que haya autores concretos que no lo hagan.

La legislación de copyright está llena de reglas por el estilo. Una de ellas es la doctrina de la «primera venta», por la cual si el lector compra este libro, puede venderlo posteriormente sin que yo, como autor, pueda imponerle restricción alguna al respecto.[36] Esta doctrina difiere, por ejemplo, de la tradición europea, donde existen «derechos morales» que conceden al creador ciertos poderes sobre el uso posterior de su obra.[37] También he mencionado ya el ejemplo de la limitación temporal de estos derechos, por la cual el creador no puede extender por más tiempo la protección que le otorga la ley (aunque el Congreso sí podría); dicha protección viene fijada por la ley y expira cuando ésta deja de ser aplicable.

Tomadas en su conjunto, estas reglas conceden al creador un control significativo —pero no perfecto— sobre el uso de aquello que produce, y al público, un cierto grado de acceso, pero no un acceso completo. El equilibrio que establecen entre estos intereses es, por lo tanto, diferente del que rige la propiedad ordinaria —en cuanto a su diseño. Estas reglas están estructuradas constitucionalmente para contribuir a construir un procomún intelectual y cultural.

---

36 La doctrina de la «primera venta» se desarrolló en el artículo 27 de la anterior *Copyright Act* (17 USC [1970]) y ha sido posteriormente adoptada en el artículo 109(a) de la actual Ley de Copyright; véase *United States vs. Goss*, 803 F2d 638 , 11º Cir, 1989 (donde se discuten ambas versiones de la ley).

37 A los europeos les gusta afirmar que estos «derechos morales» han formado parte de su sistema desde el principio de los tiempos, pero, tal y como ha demostrado el profesor Jane C. Ginsburg con respecto a Francia, éstos son en realidad una creación del siglo XIX; véase «A Tale of Two Copyrights: Literary Property in Revolutionary France and America», *Tulane Law Review*, núm. 64, 1990, p. 991.

Así pues, es la ley la que establece este equilibrio; no existiría en la naturaleza. Sin la ley, y antes del ciberespacio, los autores habrían adolecido prácticamente de protección; con la ley, cuentan con una protección significativa, pero no perfecta. En definitiva, la ley otorga a los autores algo que de otra forma no recibirían, y ello a cambio de garantizar ciertos límites en sus derechos para beneficiar al procomún intelectual en su conjunto.

Sustitutos privados para la ley pública

Si hemos afirmado que la legislación de copyright establece un equilibrio entre control y acceso, ¿qué sucede con tal equilibrio cuando el código es la ley? ¿Deberíamos esperar que éste conserve y refleje los límites que aquélla impone? ¿Qué pasará con el uso justo? ¿Y con la limitación temporal? ¿Incluirá el código privado estos «errores» en el diseño de sus protecciones?

La respuesta debería ser obvia: cuando el código protege la propiedad intelectual, nada obliga a mantener el mismo equilibrio que existía previamente. Así, nada obliga al propietario a conceder al público el derecho de uso justo. Podría hacerlo, del mismo modo que algunas librerías permiten hojear gratis sus ejemplares, pero también podría no hacerlo. El hecho de que conceda o no este derecho depende de si le reporta alguna ganancia, con lo que el uso justo queda sometido al beneficio privado. Más importante aún, dicho uso justo queda sometido al beneficio privado de los autores entendidos de forma individual, y no en su conjunto.

En consecuencia, los sistemas de confianza, como una ley privatizada, regulan en el mismo ámbito donde regula la legislación de copyright; pero, a diferencia de ésta, dichos sistemas no garantizan las mismas limitaciones sobre la protección de los derechos de autor basadas en el bien común. Los sistemas de confianza otorgan al productor el máximo control sobre los usos de una obra bajo copyright —a un precio ciertamente menor, que quizá permita que muchos más autores publiquen sus obras. Ahora bien, este poder casi perfecto que reciben los autores no se corresponde con el que les asigna la ley de derechos de autor en este ámbito. De resultas, el código desplaza el equilibrio que establece la ley al desplazar las limitaciones que ésta impone. Como escribe Daniel Benloliel:

> Los proveedores de contenido descentralizados están [...] privatizando la autoridad de aplicación de las leyes con estándares tecnológicos estrictos, con los que se prohibiría a los individuos acceder y usar un contenido digital específico de un modo que podría anular el legítimo uso justo.[38]

Hasta ahora mi descripción simplemente establece la oposición entre la ley y el código: la legislación de copyright aparece, o complementada por el código privado, o bien en conflicto con él. Puede que al lector no le convenza considerar esto como un conflicto, puesto que siempre se ha podido ejercer más control sobre una obra bajo copyright del que sancionaba la ley. Por ejemplo, si el lector posee un cuadro que está en el dominio público, nada le obliga a exponerlo públicamente. El lector podría guardarlo bajo llave en su dormitorio y no dejar que nadie lo viera jamás. En cierto sentido, el lector estaría privando así al mundo del valor de una pintura que pertenece al «dominio público», pero nadie se ha planteado nunca que esta interacción entre la ley de allanamiento y la de copyright genere un conflicto importante. Así pues, ¿por qué preocuparse si los propietarios de derechos de autor recurren al código para guardar bajo llave su contenido más allá del equilibrio establecido legalmente?

Si es en esta posición donde está situado el lector ahora mismo, déjeme que añada una parte más a esta historia. Como mencioné más arriba, la DMCA contiene una disposición que prohíbe sortear algunas medidas técnicas de protección, así como el desarrollo de herramientas destinadas a tal fin, y todo ello sin importar el propósito que tenga la elusión. De este modo, si el uso que alguien quiere hacer de una obra bajo copyright —si es que logra acceder a ella— constituye un uso justo, la DMCA sigue considerando que es un delito federal sortear las protecciones técnicas para acceder a ella. Así pues, una parte de la ley de copyright reconoce el uso justo, al tiempo que otra elimina (al menos) ciertas libertades del mismo uso justo, allá donde éste haya sido imposibilitado a través de medios técnicos.[39]

Bueno, ¿y qué si es así?, se preguntarán los escépticos. Lo que la ley da, puede también quitarlo, ¿no?

No, *no puede*, y he aquí la cuestión fundamental. Como ha indicado el Tribunal Supremo, la legislación de copyright es coherente con la Primera Enmienda sólo gracias a ciertas limitaciones importantes incluídas en ella.

---

38 Daniel Benoliel, «Technological Standards, Inc.: Rethinking Cyberspace Regulative Epistemology», *California Law Review*, núm. 92, 2004, pp. 1069, 1114.

39 Véase *Universal Studios, Inc. v. Corley*, 273 F.3d 429, 2º Cir. 2001.

Si éstas son eliminadas, entonces emergerían importantes incoherencias con la Primera Enmienda. Por consiguiente, cuando la ley se alía con el código para eliminar la protección legal del uso justo, esto debería suscitar un conflicto importante —al menos para aquéllos preocupados por mantener el equilibrio que establece la ley de copyright.

No obstante, quizá este conflicto sea algo meramente temporal. ¿No podría modificarse el código para proteger el uso justo?

La respuesta a esta pregunta esperanzada (e insisto, esperanzada, porque mi argumento principal se centra en si existen incentivos para proteger el uso justo) es que no, no directamente. El uso justo exige, de forma inherente, un juicio acerca del propósito o la intención con que se emplea una obra, lo cual queda fuera del alcance incluso de los mejores ordenadores. Ahora bien, el uso justo podría protegerse indirectamente. Un sistema que permitiera a un individuo «abrir» el sistema de confianza si sostuviera que el uso que pretende hacer es justo (acaso marcando la obra usada con una etiqueta que posibilite rastrear el uso y relacionarlo con dicho individuo), podría proteger el uso justo. O, como describe Stefik, también podría protegerse mediante un sistema que concediera a los usuarios una «licencia de uso justo» que les permitiera acceder al contenido y que respaldara la licencia con un seguro que garantizara una indemnización en caso de uso inadecuado.[40] Ahora bien, estas alternativas se apoyan de nuevo en estructuras más allá del código, puesto que sólo con éste, no hay manera de controlar adecuadamente el uso justo.

Algunos repondrán que he llegado tarde a la fiesta: la ley de copyright ya ha quedado desplazada, no por el código, sino por la ley privada que rige los contratos. Mediante el uso de de licencias de adhesión,[41] los autores están demandando cada vez más que los compradores, o los titulares de una licencia, renuncien a derechos que la ley les reconoce. Si la ley de copyright concede el derecho a aplicar la ingeniería inversa, entonces estos contratos podrían arrancar la promesa de que no se va a ejercer dicho derecho; si la ley de copyright concede el derecho a disponer del libro como desee el comprador

40 Stefik, *The Internet Edge*, *op. cit.*, pp. 99–100.

41 El autor alude en el original a las licencias *click-wrap* o *shrink-wrap*, cuyas condiciones vienen establecidas por una sola de las partes sin negociación alguna con la otra, a la que sólo se le deja la opción de aceptar o rechazar en su integridad los términos de la licencia. Los términos *click-wrap* y *shrink-wrap* se refieren a los envoltorios plásticos de los productos de software privativo, cuyas condiciones de uso estipula el fabricante de modo que el comprador tenga que asumirlas íntegramente desde el momento en que le quita el precinto al producto. [N. del E.]

después de la primera venta, estos contratos podrían exigir que el usuario renuncie a tal derecho. Y si estos términos del contrato adjunto a toda obra sujeta a derechos de autor pueden aplicarse meramente por venir «adjuntos» y ser «conocibles», entonces ya tenemos la capacidad, por medio de la ley de contratos, de rescribir el equilibrio que crea la ley de copyright.

Estoy de acuerdo en que esta carrera para privatizar la ley de copyright comenzó hace ya mucho tiempo, estimulada por decisiones como las del juez Frank Easterbrook en el caso «ProCD contra Zeidenberg». Con todo, los contratos no resultan tan perjudiciales como el código. Si un término de un contrato es incoherente con la ley de derechos de autor, podemos negarnos a obedecerlo y dejar que la otra parte recurra a los tribunales para hacerlo cumplir. En algunos casos, los tribunales se han negado de forma expresa a considerar un término contractual precisamente por ser incoherente con un principio consagrado en la ley de copyright.[42] El poder último de un contrato depende de si un tribunal decide aplicarlo o no y, aunque hoy en día los tribunales se muestran relativamente deseosos de hallar formas de aplicarlos, existe al menos la esperanza de que si la otra parte plantea su caso muy claramente, los tribunales puedan cambiar el rumbo de nuevo.[43] Como escribe Stefik, los sistemas de confianza «difieren de un contrato ordinario de forma crucial».

En un contrato ordinario, el cumplimiento de lo acordado no es automático, sino que es responsabilidad de cada una de las partes. Pueden existir disposiciones para vigilar y comprobar dicho cumplimiento, pero la responsabilidad real de actuar de acuerdo con los términos del contrato recae sobre las partes que lo suscriben. Junto a esto, la aplicación del contrato es, en última instancia, competencia de los tribunales.[44]

Esto mismo no es aplicable al código. Sean cuales sean los problemas derivados de la sustitución de la ley de copyright por la de contratos, siempre serán peores los derivados de sustituir aquélla por el código. Una vez más, ¿dónde podemos desafiar el código? Cuando el software protege sin depender del Estado, ¿dónde puedo desafiar la naturaleza de esa protección? ¿Dónde podemos exigir equilibrio cuando el código lo elimina?

---

42 Véase, por ejemplo, *People vs. Network Associates, Inc.*, 195 Misc. 2d 384, N.Y. Misc., 2003.

43 Véase William W. Fisher III, «Compulsory Terms in Internet-Related Contracts», *Chicago-Kent Law Review*, núm. 73, 1998. Fisher cataloga las restricciones que las políticas públicas imponen sobre la libertad contractual, las cuales caracteriza como «ubicuas».

44 Stefik, *The Internet Edge*, *op. cit.*, pp. 91–97.

No pretendo entrar aquí en el debate extremadamente polémico acerca de si este cambio en el modo de control resulta bueno o adecuado. Ya he escrito demasiado al respecto en otra parte.[45] Para nuestra finalidad aquí, lo importante es simplemente reconocer que se produce un cambio significativo. El código hace hoy posible un control cada vez más perfecto sobre cómo se difunde la cultura. Las regulaciones han «sido bastante coherentes [...] en dirección a expandir el poder de los propietarios para controlar el uso de sus productos».[46] Y estas regulaciones apuntan a exigir un control *perfecto* sobre cómo se difunde la cultura.

El auge del código y de los contratos que modifican la ley de copyright suscita una pregunta que dicha ley no ha tenido que responder hasta ahora. Nunca hemos tenido que elegir si se debería permitir que los autores controlaran perfectamente el uso de su propiedad intelectual, independientemente de la ley. Simplemente, tal control no era posible. El equilibrio que establecía la ley era el mejor al que podían aspirar los autores, pero ahora el código les ofrece un trato mejor. La pregunta que surge desde el punto de vista legal es si este nuevo trato proporciona algún beneficio público.

Aquí nos enfrentamos a la primera ambigüedad latente en el seno de la ley de copyright. Hay quienes sostienen que la ley ya ha zanjado esta cuestión —sea a favor o en contra del control basado en el código. A mi juicio, sin embargo, estamos ante una decisión que la ley todavía tiene que tomar. Yo tengo mis propias opiniones acerca de cuál debería ser tal decisión, pero lo que afirmo es que la tecnología nos ha obligado a enfrentarnos a una disyuntiva que no se había dado previamente. Una vez comprendido esto, podremos tomar la decisión correspondiente.

Expresado de forma más directa: siempre ha existido un conjunto de usos de las obras bajo copyright que la ley no regulaba. Incluso en el ámbito regulado, el uso justo mantenía la libertad de ciertos usos. La pregunta central es ¿por qué? ¿Se permitía la libertad de estas operaciones porque resultaba demasiado costoso controlarlas, o porque constituía un principio importante ligado al copyright?

---

45 Véase Lessig, *Free Culture: The Nature and Future of Creativity*, *op. cit.*, pp. xiv–xvi.

46 Yochai Benkler, «Net Regulation: Taking Stock and Looking Forward», *University of Colorado Law Review*, núm. 71, 2000, pp. 1203, 1254.

He aquí una cuestión que la ley nunca tuvo que resolver hasta ahora, por más que haya argumentos que respalden ambas posturas.[47] En este momento, la tecnología nos obliga a resolverla, y la pregunta es cómo lo haremos.

Un buen paralelismo con este problema lo encontramos en una parte del Derecho Constitucional. Los redactores de la Carta Magna otorgaron al Congreso el poder para regular el comercio interestatal y el comercio que influyera en éste.[48] En el momento de la fundación de EEUU, existía un importante comercio, aunque, debido a las deficiencias del mercado, no tanto como hubiera sido posible. En consecuencia, había un ámbito del comercio que los Estados eran capaces de regular.[49]

Con el tiempo, sin embargo, el alcance del comercio interestatal ha cambiado tanto que ahora hay mucho menos comercio dentro del ámbito de competencia exclusiva de los Estados. Este cambio ha producido dos clases de respuestas. Una es la de encontrar otras vías para conceder a los Estados ámbitos donde ejerzan una autoridad reguladora exclusiva. La justificación de esta respuesta se basa en la reivindicación de que dichos cambios en el comercio interestatal están destruyendo la visión del poder estatal que tenían los redactores de la Constitución.

La otra respuesta es la de reconocer el creciente alcance de la autoridad federal, pero negando que sea incoherente con el equilibrio establecido en la Constitución.[50] Ciertamente en el momento de la fundación de EEUU, parte

---

47 Véase *Campbell vs. Acuff-Rose Publishing*, 510 U.S. 569, 1994. Gordon, en «Fair use as market failure: A structural analysis of the Betamax case and its predecessors», *Columbia Law Review*, núm. 82, 1982, p. 1600, sostiene que los tribunales deberían emplear el uso justo para permitir efectuar sin compensaciones aquellas operaciones que el mercado no puede hacer; véase también Wendy J. Gordon, «On Owning Information: Intellectual Property and Restitutionary Impulse», *Virginia Law Review*, núm. 78, 1992, p. 149. En «Reality as Artifact: From Feist to Fair Use», *Law and Contemporary Problems*, núm. 55, 5PG, 1992, pp. 93-96, Gordon observa que, aunque las obras de la imaginación poseen un componente creativo, también pueden construirse a partir de hechos, los cuales han de estar ampliamente disponibles para su diseminación pública. El artículo de Gordon titulado «Toward a Jurisprudence of Benefits: The Norms of Copyright and the Problem of Private Censorship», *University of Chicago Law Review*, núm. 57, 1990, p. 1009, discute la capacidad de los titulares de derechos de autor de negar el acceso a su obra a los críticos y otras figuras; véase también Wendy Gordon, «An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory», *Stanford Law Review*, núm. 41, 1989, p. 1343.

48 Véase *Gibbons vs. Ogden*, 22 US 1, 1824 (que deroga la concesión por parte del Estado de Nueva York de un monopolio sobre la navegación de barcos de vapor por el río Hudson por estimar que es incoherente con la Ley de Costas federal de 1793); *McCulloch vs. Maryland*, 17 US 316, 1819 (donde se declara que el Congreso dispone del poder para hacer lo que sea «necesario y adecuado» para alcanzar un fin legítimo, como la regulación del comercio interestatal).

49 Véase Bernard C. Gavit, *The Commerce Clause of the United States Constitution*, Bloomington (Ind.), Principia Press, 1932, p. 84.

50 Véase *Pensacola Telegraph Company vs.Western Union Telegraph Company*, 96 US 1, 9, 1877.

del comercio no era interestatal y tampoco influía en el comercio interestatal, pero esto no implica que los redactores quisieran que siempre existiese este espacio. En lugar de ello, los redactores vincularon el alcance del poder estatal a un objetivo móvil, de modo que si este objetivo se desplaza completamente del lado del poder federal, entonces debemos aceptarlo.[51]

En ambos contextos, el cambio es el mismo. Comenzamos en una situación donde el equilibrio nos viene dado por una mezcla de fricciones en el seno de un ámbito concreto de regulación: el uso justo es un equilibrio que nos viene dado porque resulta demasiado oneroso controlar todos los usos; el poder de los Estados sobre el comercio nos viene dado porque no todas las transacciones comerciales influyen en el comercio interestatal. Cuando una nueva tecnología perturba este equilibrio, hemos de decidir si la intención original era que existiese un equilibrio o que el alcance de una de las partes se atuviera fielmente a lo que se estableció originalmente. En pocas palabras, ambos contextos plantean ambigüedades.

Muchos observadores (entre los que me incluyo) se inclinan vehementemente por una opción o por otra. En este sentido, creemos que esta ambigüedad latente no constituye en realidad ambigüedad alguna. En el contexto del poder federal, creemos que, o bien se concebía que los Estados debían mantener un ámbito exclusivo de autoridad,[52] o bien que el gobierno federal debía tener todos los poderes sobre el comercio interestatal.[53] En el contexto del uso justo, creemos que, o bien éste representa un mínimo de uso público garantizado

---

51 Como un comentarista lo expresó a comienzos del siglo XX: «Si el poder del Congreso posee una incidencia mayor en 1918 de la que podía tener en 1789, ello se debe meramente a que la producción depende ahora más que entonces de mercados extraestatales. Ningún Estado vive hoy tan aislado como lo hacía hace un siglo. Lo que está cambiando no es nuestro sistema de gobierno, sino nuestra organización económica», Thomas Reed Powell, «The Child Labor Law, the Tenth Amendment, and the Commerce Clause», *Southern Law Quarterly*, núm. 3, 1918, pp. 175, 200–201.

52 Véase Alexis de Tocqueville, *Democracy in America*, vol. 1, Nueva York, Vintage, 1990, pp. 158–170, sobre la idea de que el diseño de los redactores de la Constitución estadounidense empujaba a los Estados a legislar en un ámbito amplio y a mantener activo el gobierno local [ed. cast.: *La democracia en América*, trad. por Raimundo Viejo Viñas, Madrid, Akal, 2007].

53 Véase *Maryland vs.Wirtz*, 392 US 183, 201, 1968; voto particular del juez William O. Douglas: la decisión de la mayoría de incluir dentro de la cláusula comercial a los empleados de empresas de propiedad estatal constituía «una invasión tan grave de la soberanía de los Estados, protegida por la Décima Enmienda, que [resultaba] incoherente con nuestro federalismo constitucional». *State Board of Insurance vs. Todd Shipyards Corporation*, 370 US 451, 456, 1962; donde se mantiene que «el poder del Congreso para conceder o retirar su protección al comercio interestatal contra la regulación o la introducción de impuestos por parte de los Estados es tan completa que sus ideas acerca de las políticas en este ámbito deberían prevalecer»).

independientemente de la tecnología,[54] o bien que no es más que un acuerdo eficaz que se adopta en respuesta a una tecnología ineficaz, y que, en consecuencia, ha de ser eliminado en cuanto se pueda alcanzar la eficacia.

En ambos casos, no obstante, estas posturas pueden plantear el problema de forma demasiado simple. Puede que la mejor respuesta en ambos contextos sea que la cuestión quedase sin resolver en su momento: quizá nadie pensó en ella y, por lo tanto, no existe una respuesta a la pregunta de qué habrían decidido los redactores de la Constitución si hubiera variado algún presupuesto fundamental. Y si esto es así, hemos de ser nosotros quienes resolvamos la cuestión según nuestro propio criterio. Como afirma Stefik acerca de los sistemas de confianza —y podría esperarse que también acerca de sus implicaciones—: «Se trata de una herramienta que ni los creadores de la ley de copyright ni aquéllos que creen que las leyes que rigen la propiedad intelectual no pueden aplicarse jamás imaginaron».[55]

La pérdida del uso justo es una consecuencia de la perfección de los sistemas de confianza. Que el lector considere que dicha pérdida representa o no un problema depende de su visión del principio del uso justo. Si el lector considera que se trata de un principio público que debería existir independientemente del régimen tecnológico, entonces la aparición de esta mejora debería preocuparle. Desde ese punto de vista, había un principio latente en la imperfección del antiguo sistema que ahora ha sido eliminada.

Pero incluso si el lector no considera que dicha pérdida represente un problema, los sistemas de confianza amenazan otros principios latentes en la imperfección del mundo real. A continuación analizaremos el segundo de ellos.

---

54 Véase Michael G. Frey, «Unfairly Applying the Fair Use Doctrine: *Princeton University Press vs. Michigan Document Services*, 99 F3d 1381, 6º Cir 1996», *University of Cincinnati Law Review*, núm. 66, 1998, pp. 959, 1001; Frey afirma que «la protección del copyright existe primordialmente para beneficio del público, no de los autores individuales. La ley de copyright les concede a éstos un beneficio considerable en términos del derecho monopolístico a controlar sus creaciones, pero ese derecho existe únicamente para asegurar la creación de nuevas obras. La doctrina del uso justo es una importante válvula de seguridad que garantiza que el beneficio de los autores individuales no sobrepasa al del público»; Marlin H. Smith («The Limits of Copyright: Property, Parody, and the Public Domain», *Duke Law Journal*, núm. 42, 1993, pp. 1233, 1272) afirma que «la ley de copyright se comprende mejor como el equivalente a un guardián que controla el acceso a las obras sujetas a derechos de autor, pero que garantiza, mediante el uso justo, cierto grado de disponibilidad pública de la obra».

55 Stefik, «Letting Loose the Light», *op. cit.*, p. 244. Para una aplicación excelente del análisis general de *El código* a fin de defender que el análisis específico de este capítulo es errónea, véase John Tehranian, «All Rights Reserved? Reassessing Copyright and Patent Enforcement in the Digital Age», *University of Cincinnati Law Review*, núm. 72, 2003, p. 45.

El anonimato que permite la imperfección

Durante algunos años estuve estudiando en una universidad de Inglaterra. En el campus, había una «bodeguilla» —una tienda dentro del campus que, básicamente, vendía alcohol. Durante la primera semana que pasé allí tuve que comprar una gran cantidad de botellas de whisky escocés (regalos poco imaginativos para familiares y amigos, que yo recuerde). Una semana después de efectuar estas compras, recibí una citación para presentarme en el despacho de mi tutor a hablar con él. Cuando acudí a su despacho, el tutor me interrogó acerca de mis compras, pues estimaba que se trataba de una cantidad excesiva de alcohol, y quería saber si yo tenían una buena razón para comprarla.

Ni que decir tiene que la pregunta me dejó estupefacto. Por supuesto, técnicamente, había realizado una compra en el campus sin preocuparme de ocultar mi identidad (de hecho, lo había cargado a mi cuenta universitaria), con lo que, formalmente, había revelado los detalles de mis compras a la universidad y a sus agentes. Con todo, me sorprendió que esta información fuera controlada y posteriormente investigada por las autoridades universitarias. Podía entender por qué lo hacían, y también el bien que podía desprenderse de ello, pero nunca hubiera imaginado que tal información llegara a emplearse de ese modo.

Si aquello constituía una invasión, no cabe duda de que era más bien pequeña. En adelante me resultó bastante sencillo ocultar mis borracheras simplemente comprando el alcohol en la licorería local que estaba fuera del campus. (Aunque después me enteré de que era la universidad la que alquilaba el local a esta licorería, por lo que ¿quién sabe a qué tratos habrían llegado?). Y, en cualquier caso, no recibí castigo alguno, sino que mi tutor se limitó a manifestarme su preocupación. Ahora bien, este ejemplo sugiere una idea más general: cotidianamente revelamos al mundo cierta clase de información acerca de nosotros mismos que esperamos que el mundo no utilice, pero ¿qué sucede si lo hace?

Los sistemas de confianza dependen de este tipo de información —dependen de la capacidad de saber cómo utiliza la gente la propiedad que está siendo protegida. Para establecer sus tarifas de un modo más efectivo, el sistema debería conocer idealmente lo más posible acerca de los individuos y de sus hábitos de lectura. Necesita conocer esta información porque necesita encontrar una vía eficaz para seguir la pista del uso de las obras y, así, poder cobrar por ello.[56]

---

56 Utilizo el término eficaz tanto en el sentido de que sea barato seguir la pista al uso como de que también lo sea discriminar la tarifa que le corresponde; William W. Fisher III, «Property and Contract on the Internet», *Chicago-Kent Law Review*, núm. 74, 1998.

Sin embargo, este seguimiento implica incurrir en una cierta invasión. Vivimos en un mundo donde pensamos acerca de lo que leemos del mismo modo en que yo pensaba acerca de lo que compré en el campus de Inglaterra —no esperamos que nadie esté efectuando un seguimiento al respecto. Y nos quedaríamos tan estupefactos como me quedé yo si nos enterásemos de que la biblioteca estuviera controlando los libros que consulta la gente y empleando dicha información con algún propósito de vigilancia.

Pues bien, este tipo de seguimiento es precisamente el que requieren los sistemas de confianza, con ello surge la siguiente pregunta, una pregunta que posee un cierto paralelismo con la cuestión del uso justo: ¿debería existir un derecho contra esta forma de vigilancia? En un mundo donde dicha vigilancia no podía darse en la práctica, está claro que no existía un derecho que protegiera de ella. Pero ahora que puede darse, hemos de preguntarnos si el derecho latente a leer anónimamente, que antes nos venía dado por las imperfecciones tecnológicas, debería constituir un derecho protegido por la ley.

Julie Cohen defiende que sí, y podemos entender claramente cómo se desarrolla su argumentación.[57] Sea cual sea su fuente, constituyen principios de este mundo que podamos explorar intelectualmente por nuestra cuenta y que podamos leer de forma anónima sin temer que los demás se enteren, nos vigilen o cambien su actitud hacia nosotros por ello. Éste es un elemento de la libertad intelectual, una parte de lo que somos.[58]

Ahora bien, este elemento puede ser eliminado por los sistemas de confianza, que necesitan efectuar una vigilancia que destruye nuestro anonimato. Así pues, hemos de decidir si conservamos los principios del presente en un contexto de sistemas de confianza, y en caso afirmativo, cómo lo hacemos.

---

57 Julie E. Cohen, «A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace», *Connecticut Law Review*, núm. 28, 1996: leer de forma anónima está «tan íntimamente conectado con las libertades de expresión y pensamiento que la Primera Enmienda debería interpretarse de modo que garantice tal derecho» (pp. 981, 982). Cohen ha extendido su análisis al contexto de las tecnologías que no recopilan información privada. Véase Julie E. Cohen, «DRM and Privacy», *Berkeley Technology Law Journal*, núm. 18, 2003, p. 575. Véase también Helen Nissenbaum, «Securing Trust Online: Wisdom or Oxymoron», *Boston University Law Review*, núm. 81, 2001, p. 635, donde describe la dinámica de confianza que estos incipientes sistemas evocarán. Para obras relacionadas, de gran contundencia, véase Sonia K. Katyal, «The New Surveillance», *Case Western Reserve Law Review*, núm. 54, 2003, p. 297.

58 «La libertad de leer anónimamente constituye una parte fundamental de nuestra tradición, y la elección de los materiales de lectura es tan expresiva de nuestra identidad como la decisión de usar u ocultar nuestro nombre» (Cohen, «A Right to Read Anonymously», *op. cit.*, p. 1012).

En principio, podríamos estar ante una cuestión de traducción: a saber, ¿cómo deberían adaptarse los cambios tecnológicos para conservar los principios de un contexto anterior en otro nuevo? Se trata de la misma cuestión que planteó Brandeis acerca de las escuchas telefónicas,[59] la misma a la que responde el Supremo continuamente en decenas de contextos. Se trata fundamentalmente de una cuestión acerca de cómo conservar una serie de principios cuando varían los contextos.

En los contextos del uso justo y de la lectura, Cohen ha formulado una respuesta coherente a esta pregunta sobre la traducción. Ella defiende que existe el derecho a resistirse, o de efectuar un *hacking* de los sistemas de confianza en la medida en que estos infrinjan el derecho tradicional de uso justo. (Hay quien ha llamado a esta postura el «Teorema de Cohen»). En cuanto a la lectura, Cohen sostiene que los esquemas de gestión de derechos de autor deben proteger el derecho a leer anónimamente —si éstos vigilan, han de construirse para que respeten el anonimato. La estrategia es la misma: Cohen identifica un principio propiciado por una arquitectura antigua, y ahora amenazado por otra nueva, y acto seguido aboga por el derecho afirmativo a proteger el principio original.

Sin embargo, de nuevo aquí podríamos enfocar la cuestión de un modo más ambiguo. Yo comparto la postura de Cohen, pero el argumento opuesto no es desdeñable. Si se permite emplear la tecnología para hacer disponibles las obras bajo copyright, ¿por qué no se permite recopilar información acerca de quién usa qué obras? Dicha recopilación no forma parte del propio copyright, sino que es un subproducto de la tecnología. Y dado que nuestra tradición nunca ha tenido antes esta capacidad técnica, es difícil afirmar que en el pasado se tomó una decisión al respecto.

Cultura del permiso contra cultura libre

Ya he descrito las limitaciones que la legislación de copyright se impone a sí misma. Además, he sostenido que tales limitaciones reflejan principios importantes y expresan el equilibrio que dicha legislación trata de alcanzar.

59 Véase *Olmstead vs. United States* 277 US 438, 474, 1928; voto particular del juez Louis Brandeis: «¿Es posible que la Constitución no prevea ninguna protección contra tales invasiones de la seguridad individual?».

Pero en este debate se echa de menos demasiado a menudo, el sentido esencial de la perspectiva. Nos centramos en las modificaciones graduales de la ley y perdemos de vista el sentido profundo en que ha cambiado su significado.

Este cambio viene producido por la interacción imprevista entre la arquitectura de las tecnologías digitales y la arquitectura de la ley.

La ley de copyright regula esencialmente las «copias». En el mundo analógico, existían muy pocos contextos donde se produjeran «copias». Como describió Jessica Litman hace más de una década:

> A comienzos del siglo XX, la ley estadounidense de copyright resultaba muy técnica, incoherente y difícil de comprender, pero no se aplicaba a mucha gente o a muchas cosas. Si alguien era autor o editor de libros, mapas, gráficos, pinturas, esculturas, fotografías o partituras, o dramaturgo o productor teatral, o impresor, entonces la ley de copyright le afectaba. En cuanto a los libreros, editores fonográficos o de rollos de pianola, los productores cinematográficos, los músicos, los eruditos, los congresistas y los consumidores ordinarios, todos ellos podían dedicarse a sus asuntos sin toparse jamás con ningún problema relativo a derechos de autor.[60]

Así pues, existían muchas maneras de usar las obras creativas en el mundo analógico que no implicaban producir una copia.

La tecnología digital, en esencia, realiza copias. Así, las copias son a la vida digital lo que la respiración es a nuestra vida física. En un contexto digital no hay forma de usar un contenido sin que ello conlleve producir una copia. Cuando leemos un libro almacenado en nuestro ordenador, realizamos una copia (al menos en la memoria RAM, para poder *pasar las hojas*). Hagamos lo que hagamos con el contenido digital, técnicamente estamos produciendo una copia.

Este hecho técnico de las tecnologías digitales, unido a la arquitectura técnica de la ley, produce un cambio profundo en el alcance de la ley de copyright que demasiada gente pasa por alto: mientras que en el mundo analógico la vida transcurría al margen de dicha ley, en el digital, la vida está sometida a ella. Por ende, la ley de derechos de autor se

---

60 Véase Jessica Litman, «The Exclusive Right to Read», *Cardozo Arts and Entertainment Law Journal*, núm. 13, 1994, p. 29.

aplica a todos los actos de nuestra vida allí. Cada uno de los usos que realizamos, o bien está sometido a los términos de una licencia, o bien es ilegal, a menos que se lo considere un uso justo. Así pues, la aparición de las tecnologías digitales ha expandido radicalmente el ámbito de aplicación de la ley de copyright —que pasa de regular una porción minúscula de la vida humana a regular cada bit de vida que hay en un ordenador.

Por supuesto, si el lector piensa exclusivamente en proteger la distribución de la cultura creada profesionalmente, puede que esto no le preocupe demasiado. Si el lector trata de erradicar la «piratería», un régimen que establece que hay que pedir permiso por cada uso que se haga de una obra es un régimen que le proporciona una amplia gama de herramientas para eliminar la piratería.

Sin embargo, aunque nadie lo diría al escuchar los debates actuales en torno al copyright, la protección de la distribución de la cultura creada profesionalmente no es, de hecho, el único componente de la cultura, y estimo que ni siquiera el más importante. Es más, desde un punto de vista histórico, la cultura producida profesionalmente, de arriba a abajo, no supone más que una ínfima parte de lo que hace de cualquier cultura lo que es. Acaso el siglo XX haya constituido una excepción a esta regla, pero ningún Congreso ha sometido a votación convertir la cultura profesional en la única cultura legal en el seno de nuestra sociedad.

Y es que, junto a esta cultura profesional, existe una cultura amateur —donde el término *amateur* no significa inferior o carente de talento, sino más bien creada por gente que no la produce por dinero, sino por *amor* a la cultura. En este sentido, la cultura amateur se encuentra por doquier —en la mesa de nuestra cocina, donde nuestro padre o nuestra hermana cuentan chistes basados en el último escándalo político, o en el último programa satírico; en el sótano de casa, donde nuestro hermano y sus tres mejores amigos se provocan daños permanentes en los tímpanos mientras tratan de convertirse en los próximos Rolling Stones; en los vecinos que se reúnen todos los jueves y domingos para cantar en el coro de la iglesia; en la escuela del barrio, donde niños y profesores crean arte y música mientras aprenden acerca de nuestra cultura; y en los alumnos de dicha escuela, que deshilachan sus pantalones o llevan sus camisetas de un modo original, como un medio de expresión y creación cultural.

Esta cultura amateur siempre nos ha acompañado, si bien hoy día sigue presente de forma «encubierta»,[61] como señalan Dan Hunter y Greg Lastowska. Es justamente así cómo se desarrolla la imaginación de los niños,[62] y, más aún, cómo se ha desarrollado siempre la cultura. Como escribe Siva Vaidhyanathan:

> La producción cultural democrática y diseminada (la producción P2P, como podría denominarse) [...] meramente se hace eco del modo en que los textos culturales han circulado y han sido revisados por comunidades discursivas en todas partes a lo largo de los siglos. Los textos a menudo son sometidos a un proceso similar al juego del «teléfono», en el que un texto es distorsionado sustancialmente —a veces incluso sin querer— a través de múltiples revisiones pequeñas. [...] Estas revisiones textuales tan radicales se han dado en otros contextos y han contribuido a desarrollar críticas políticas, cuando no movimientos políticos. Por ejemplo, en el contexto de EEUU, el historiador Lawrence Levine (1988) ha documentado cómo los actores de clase obrera y las audiencias del siglo XIX revisaban las obras de William Shakespeare, adaptándolas a sus contextos, preocupaciones e ideologías locales. Y el historiador Eric Lott (1993) ha explicado cómo *La cabaña del Tío Tom* fue reelaborada por las comunidades blancas de clase obrera para contribuir a la causa de la dominación racial en lugar de al mensaje de liberación cristiana al que pretendía servir el libro.[63]

También resulta importante que esta forma de remezcla cultural ha estado históricamente libre de regulación. Nadie pensaría que cuando cuenta un chiste en la mesa, entona una canción con sus amigos o ensaya con ellos para convertirse en los próximos Rolling Stones, necesita tener cerca a un abogado para que le aclare sus derechos a «usar» la cultura. Históricamente, la ley de copyright se ha centrado en la vida comercial, dejando al margen de su regulación legal la creatividad no comercial, o aquélla que va más allá de lo comercial.

---

61 Véase Dan Hunter y F. Gregory Lastowka, «Amateur-to-Amateur», *William and Mary Law Review*, núm. 46, diciembre de 2004, pp. 951, 1026–27.

62 Lasica, *Darknet: Hollywood's War Against the Digital Generation*, *op. cit.*, p. 18: «El director del Programa de Estudios Comparativos de Medios del MIT y autor de nueve libros sobre cultura popular, [Henry] Jenkins, afirma que desde una edad temprana los niños reelaboran imaginativamente lo que se puede hacer con los personajes y escenarios del cine y la televisión. Estos niños se divierten con videojuegos con los que pueden controlar un personaje dentro de unos límites, permitiendo los juegos más recientes un repertorio aún mayor de interactividad y de comportamientos. Cuando se conectan a la Red, pueden compartir sus historias, encontrándose hasta niños de siete años que publican en los sitios de ficción relatos simples, pero interesantes, sobre Harry Potter y Pokemon».

63 Siva Vaidhyanathan, «Remote Control: The Rise of Electronic Cultural Policy», *Annals of the American Academy of Political and Social Science*, vol. 597, núm. 1, 1 de enero de 2005, p. 126.

Ahora todo esto ha cambiado y las tecnologías digitales son las responsables de ello. En primer lugar, lo más importante es que las tecnologías digitales han expandido radicalmente el alcance de esta cultura amateur. En la actualidad, la remezcla ingeniosa de algún acontecimiento político o de la última canción de nuestro grupo favorito ha dejado de ser algo que sólo podemos compartir entre amigos. Las tecnologías digitales han simplificado la captura y compartición de esta creatividad con el mundo entero. La diferencia más importante entre la Internet de 1999 y la actual es la explosión de creatividad generada por los usuarios — desde los *blogs* a las emisiones de *podcast* y *videocast* y las remezclas de contenidos [*mashups*], la Internet de hoy constituye un espacio de extraordinaria creatividad.

En segundo lugar, las tecnologías digitales han democratizado la creatividad, proporcionando a un amplio abanico de creadores potenciales la capacidad de realizarse. «La gente está saliendo del coma consumista», describe un comentarista.[64] Como DJ Danger Mouse expresó en el Congreso Web 2.0 de 2004:

> Remezclar es muy fácil. Necesitas años para aprender a tocar la guitarra y a componer tus propias canciones, pero sólo unas pocas semanas de práctica con una mesa de mezclas para hacer que la gente baile y sonría, y sólo unas pocas horas para ensamblar algo bueno con el software adecuado. Con una barrera de entrada tan baja, todo el mundo da el salto y comienza de inmediato a ser creativo.[65]

En tercer lugar, y en relación directa con el relato de este capítulo, en la medida en que esta creatividad se expresa a través de la red, queda ahora sometida a la ley de copyright. De esta forma, en la medida en que usa la creatividad ajena, es necesario el permiso ajeno; en la medida en que se construye sobre la creatividad ajena, es necesario asegurarse de que es legal hacer tal cosa. Así, se ha implantado todo un sistema de regulación sobre la base de una economía de la creatividad que jamás había sido regulada hasta ahora. La cultura amateur, la cultura construida desde abajo, la cultura que vive al margen de transacciones comerciales —toda ella está hoy regulada de una forma que no existía hace 30 años.

---

64 Lasica, *Darknet: Hollywood's War Against the Digital Generation*, *op. cit.*, p. 78, citando a Ernest Miller.

65 Extracto de «Music Is a Platform», intervención de DJ Danger Mouse en el Congreso Web 2.0 6 de octubre de 2004, citado en Lasica, *Darknet: Hollywood's War Against the Digital Generation*, *op. cit.*, p. 211.

Un ejemplo reciente de este conflicto permite explicar la idea muy concisamente. Hay un género de creatividad digital llamado *Anime Music Videos* (AMV). Los AMV son videos musicales basados en remezclas de secuencias de *anime* y canciones. Muchos chicos dedican cientos de horas, a veces miles, a editar los dibujos *anime* de modo que encajen perfectamente con la música elegida. El resultado es, en una palabra, extraordinario, representando uno de los usos más creativos de la tecnología digital que haya visto.

Por más que la dimensión de este género creativo no sea reducida, tampoco es enorme. Básicamente un sitio domina la actividad en torno a los AMV, congregando a más de medio millón de miembros y a unos 30.000 creadores que cuelgan sus videos musicales de *anime*.

En noviembre de 2005 un prominente sello discográfico, Wind-Up Records, informó al sitio web de que quería que fueran eliminados de él todos los AMV que contuvieran canciones de artistas de Wind-Up Records. Ello implicaba eliminar unos 3.000 videos, que representaban al menos 250.000 horas de trabajo voluntario de creadores de todo el mundo —trabajo que sólo produciría un efecto real: promocionar la obra de los artistas en cuestión.

Desde una perspectiva estrictamente legal, se trata de un caso sencillo. Los chavales que crean AMV están generando una obra derivada a partir del *anime*, están distribuyendo copias íntegras de las canciones empleadas y están sincronizando el video y la música —todo ello sin el permiso de los propietarios del copyright.

Pero desde la perspectiva de la cultura, éste debería ser un caso muy delicado. La creatividad manifestada por este trabajo es extraordinaria. No puedo mostrársela al lector en un libro, pero las notas le remiten a un ejemplo que puede consultar.[66] Se trata de un trabajo creativo amateur de carácter no comercial —justamente el tipo de trabajo que jamás ha estado sometido a la regulación legal, pero que ahora, al vivir en un contexto digital, es vigilado y regulado por medio de la ley.

También en este caso tengo mis firmes convicciones acerca de cuál debería ser la respuesta correcta a este caso, pero antes debemos reconocer la ambigüedad latente que plantea este conflicto.

---

66 Véanse, por ejemplo, los videos musicales de *anime* disponibles en http://www.animemusicvideos.org/home/home.php.

Debido a los cambios en la tecnología digital, ahora la ley puede regular todos los usos de las obras creativas en un entorno digital. A medida que la vida se vaya desplazando progresivamente hacia dicho entorno, la ley regulará cada vez más los usos de la cultura.

¿Es esto coherente con nuestros principios?

Una vez más, la respuesta podría buscarse en primer lugar tratando de traducir los principios fundamentales al contexto actual. Desde esa perspectiva, resulta extremadamente complicado imaginar que la visión de los fundadores incluyera el nivel de regulación legal que el régimen actual abarca.

Y una vez más, podría cuestionarse tal conclusión reconociendo que en aquella época no existía la posibilidad de una regulación tan extensiva, por lo que no se podía plantear la opción de si debería o no ser permitida. Cuando se tome esta decisión, debería reconocerse que, al mismo tiempo que se aplica a la cultura amateur una regulación inédita y extensiva, esa misma regulación genera nueva riqueza para la cultura profesional. En consecuencia, hemos de decidir qué forma de cultura deberíamos proteger. Se trata de una decisión que aún no se ha tomado de forma directa, otra decisión que nos corresponde tomar a nosotros.

Los problemas que plantea la perfección.

Estos tres ejemplos revelan un conflicto común —que llegara mucho más allá del copyright. Hubo una época en que disfrutamos de un cierto tipo de libertad, una libertad que no era fruto de una elección directa, sino más bien de los altos costes que acarreaba el control.[67] Ésta fue la conclusión a la que llegamos con respecto al uso justo —que cuando el coste del control era elevado,

---

67 Peter Huber se basa explícitamente en los altos costes del control en su refutación de *1984*, de Orwell; véase *Orwell's Revenge: The 1984 Palimpsest*, Nueva York, Maxwell Macmillan International, 1994. Ahora bien, ésta es una fundamentación débil sobre la que construir la libertad, especialmente a medida que disminuye el coste del control por medio de redes. Frances Cairncross también desafía esta idea de forma efectiva en *The Death of Distance: How the Communications Revolution Will Change Our Lives*, Boston, Harvard Business School Press, 1997, pp. 194–95 [ed. cast.: *La muerte de la distancia: cómo la revolución de las comunicaciones cambiará la vida de la empresa*, trad. por Laura Traffi, Barcelona, Ediciones Paidós Ibérica, 1998].

el espacio para el uso justo era muy amplio. Esto mismo sucedía con la lectura anónima: en el espacio real leemos anónimamente no tanto porque las leyes protejan ese derecho como porque el coste de controlar lo que leemos es desmesurado. Y lo mismo se aplicaba a la cultura amateur: floreció libre de regulación porque ésta no podía alcanzarla fácilmente.

Ahora bien, cuando se reducen los costes del control, la libertad se ve amenazada. Esta amenaza nos obliga a tomar una decisión —¿permitimos la erosión de una libertad previa o construimos otras limitaciones para recrear esa libertad original?

La ley de propiedad intelectual constituye el primer ejemplo de este argumento general. A medida que cambie la arquitectura de Internet, ésta permitirá una protección de la propiedad intelectual mayor de la que permitía la arquitectura del espacio real; esta protección ampliada nos obligará a tomar una decisión a la que no tenemos que enfrentarnos en el espacio real. ¿Debe permitir esa arquitectura un control perfecto sobre la propiedad intelectual, o debemos incluir en ella una imperfección que garantice un cierto grado de uso público o un cierto espacio para la libertad individual?

Ignorar estos interrogantes no hará que desaparezcan. Fingir que los redactores de la Constitución los respondieron tampoco es ninguna solución. En este contexto (y éste es sólo el primero), necesitaremos formular un juicio de valor acerca de qué principios tendrá que proteger la arquitectura.

Decisiones

He afirmado anteriormente que el ciberespacio planteará tres opciones importantes en el contexto de la propiedad intelectual: si se permite que la propiedad intelectual se convierta de hecho en una propiedad absoluta (porque esto es precisamente lo que haría un régimen de protección de la propiedad intelectual basado en un código perfecto); si se permite que este régimen elimine el anonimato subyacente en arquitecturas de control menos eficaces; y si se permite que la expansión de la propiedad intelectual asfixie la cultura amateur. Tales decisiones no fueron tomadas en su momento por los redactores de la Constitución, por lo que somos nosotros quienes debemos hacerlo ahora.

Yo tengo mi propia opinión al respecto, en este contexto y en los tres que analizaré a continuación. Pero soy abogado, y a los abogados nos enseñan a apuntar hacia otro lado —hacia los redactores de la Constitución, hacia la Carta de las Naciones Unidas, hacia una ley promulgada por el Congreso— cuando discutimos acerca de cómo deberían ser las cosas. Al haber afirmado que no existe una autoridad equivalente en este ámbito, siento como si debiera guardar silencio.

No obstante, habrá quien atribuya este silencio a mi cobardía y sostenga que debería exponer lo que pienso. Así pues, en cada una de estos tres contextos (propiedad intelectual, privacidad y libertad de expresión), ofreceré mi opinión acerca de cómo deberíamos tomar tales decisiones. No obstante, hago esto en cierta medida bajo coacción e invito al lector a que se limite a ignorar mis convicciones. Éstas serán breves, sumarias, fáciles de desechar. Lo que deseo subrayar realmente se halla en el resto del libro —siendo lo más importante llegar a comprender que nos corresponde tomar decisiones.

Anonimato

A mi juicio, Julie Cohen tiene toda la razón por lo que respecta al anonimato y, en este sentido, el «Teorema de Cohen» me resulta muy inspirador. Por muy eficaz que pueda ser la alternativa, deberíamos diseñar el ciberespacio de modo que se garantice de entrada el anonimato —o, para ser más preciso, la posibilidad de emplear *seudónimos*. Si el código va a vigilar lo que yo hago, al menos no debería saber quién es ese «yo» al que vigila. Si el código averigua que «14AH342BD7» lee tal libro y tal otro, eso me quita un peso de encima; pero si puede vincular ese número con mi nombre, eso ya me inquieta profundamente.

Cohen también tiene razón por un segundo motivo: todo el bien que produce la vigilancia podría alcanzarse protegiendo también la privacidad. Puede que el diseño de rutinas que rompan la rastreabilidad requiera un poco más de trabajo de codificación y puede que garantizar la protección de la privacidad requiera una mayor planificación. Pero si estas reglas se introducen en el diseño del ciberespacio de forma abierta, su coste no sería excesivamente alto. Resulta mucho más barato diseñar ahora protecciones de privacidad que actualizar luego la arquitectura para incorporarlas.

El procomún

Entiendo el procomún como un recurso que cualquier persona de una comunidad relevante puede usar sin pedir permiso a nadie. Puede que no necesite ese permiso porque el recurso no está sometido a ningún control legal (porque, en otras palabras, está en el dominio público); o puede que no lo necesite porque ya ha sido concedido por anticipado. En uno u otro caso, el único requisito para usar el recurso o utilizarlo como base para otro trabajo es tener acceso a él.[68]

En este sentido, los interrogantes acerca del alcance de la ley de copyright plantean si en nuestro futuro se protegerá el procomún intelectual que se protegía en el pasado. Insisto una vez más en que dicha protección provenía del hecho de que el control suponía un coste demasiado grande. Pero ahora que tal coste se ha eliminado, ¿conservaremos o destruiremos el procomún que existía?

Mi opinión es que deberíamos conservarlo.

Podemos diseñar el ciberespacio para conservarlo o para destruirlo. (Thomas Jefferson pensaba que la naturaleza ya había impuesto su arquitectura, pero concibió sus escritos antes de que existiera el código). Deberíamos optar por diseñarlo con la presencia del procomún. Nuestro pasado poseía espacios comunales que no podían destruirse mediante el diseño; dichos espacios fueron muy valiosos para el desarrollo de nuestra cultura. Apenas estamos comenzando a vislumbrar lo valioso que el procomún del futuro puede llegar a ser para nosotros. Los eruditos en el campo de la propiedad intelectual lo captaron —mucho antes de que surgiera el ciberespacio— y pusieron los cimientos de gran parte del debate que hemos de abordar ahora.[69] Las obras más eminentes del ciberderecho provienen del ámbito de la propiedad intelectual. En un amplio abanico de contextos, estos eruditos han formulado una poderosa defensa del valor sustantivo del procomún intelectual.[70]

---

68 Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World*, *op. cit.*, pp. 19–23.

69 Una obra fundamental es David Lange, «Recognizing the Public Domain», *Law and Contemporary Problems*, núm. 44, 1981, p. 147. No obstante, existen muchos precedentes importantes que fundamentan este argumento. Véase, por ejemplo, Benjamin Kaplan, *An Unhurried View of Copyright*, Nueva York, Columbia University Press, 1967 y los artículos de Wendy J. Gordon citados en la nota 47.

70 En la primera edición de este libro, además de a la obra de Boyle, manifestaba ampliamente mi reconocimiento a aquellas obras que han formado mis concepciones, incluyendo Keith Aoki, «Foreword to Innovation and the Information Environment: Interrogating the

James Boyle lo hace de modo contundente en su extraordinario libro *Shamans, Software, and Spleens*.[71] Poniendo en relación cuestiones relativas al ciberespacio y al espacio real, Boyle desmenuza los desafíos a los que nos

Entrepreneur», *Oregon Law Review*, núm. 75, 1996, p. 1; en «(Intellectual) Property and Sovereignty», *op. cit.*, Aoki aborda los desafíos al concepto tradicional de propiedad que surgen del crecimiento de la tecnología digital de información; en «Authors, Inventors, and Trademark Owners: Private Intellectual Property and the Public Domain», *Columbia-VLA Journal of Law and the Arts*, núm. 18, 1993, p. 1, observa las limitaciones cambiantes de la legislación de propiedad intelectual entre los ámbitos de información «públicos» y «privados», y defiende que la tendencia a incrementar el número de derechos exclusivos de los autores está convirtiendo el dominio público en propiedad intelectual privada, y está restringiendo otros usos de las obras de expresión, socialmente valiosos, que no se ajustan al modelo de «autoría» subyacente en las tradiciones estadounidenses de copyright; también defiende que la reciente expansión de la legislación relativa a las marcas registradas ha permitido a sus propietarios obtener derechos de propiedad sobre las marcas que no respetan el objetivo de la Ley Lanham de evitar la confusión del consumidor. Benkler, «Free as the Air to Common Use», *op. cit*. Yochai Benkler, «Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment», *Harvard Journal of Law and Technology*, núm. 11, 1998, p. 287. Julie E. Cohen, «Copyright and the Jurisprudence of Self-Help», *Berkeley Technology Law Journal*, núm. 13, 1998, p. 1089; Julie E. Cohen, «Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"», *Michigan Law Review*, núm. 97, 1998, p. 462; Julie E. Cohen, «Some Reflections on Copyright Management Systems and Laws Designed to Protect Them», *Berkeley Technology Law Journal*, núm. 12, 1997, pp. 161, 181–182; Julie E. Cohen, «Reverse-Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs», *Southern California Law Review*, núm. 68, 1995, p. 1091. Niva Elkin-Koren, «Contracts in Cyberspace: Rights Without Laws», *Chicago-Kent Law Review*, núm. 73, 1998; Niva Elkin-Koren, «Copyright Policy and the Limits of Freedom of Contract», *Berkeley Technology Law Journal*, núm. 12, 1997, pp. 93, 107–110, donde critica la sentencia del caso «ProCD»; Niva Elkin-Koren, «Cyberlaw and Social Change: A Democratic Approach to Copyright Law in Cyberspace», *Cardozo Arts and Entertainment Law Journal*, núm. 14, 1996, p. 215; en «Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators», *Cardozo Arts and Entertainment Law Journal*, núm. 13, 1995, pp. 345, 390–399, Elkin-Koren analiza los problemas creados por la aplicación de la ley de copyright en un entorno digitalizado. En «Goodbye to All That—A Reluctant (and Perhaps Premature) Adieu to a Constitutionally Grounded Discourse of Public Interest in Copyright Law», *Vanderbilt Journal of Transnational Law*, núm. 29, 1996, p. 595, Peter A. Jaszi aboga por el desarrollo de nuevos argumentos basados en políticas públicas, así como de razonamientos fundamentados en la Constitución con el fin de combatir las tendencias legislativas y judiciales que expanden el copyright y reducen el acceso público al «procomún intelectual»; véase también Peter A. Jaszi, «On the Author Effect: Contemporary Copyright and Collective Creativity», *Cardozo Arts and Entertainment Law Journal*, núm. 10, 1992, pp. 293, 319–20; Peter A. Jaszi, «Toward a Theory of Copyright: The Metamorphoses of "Authorship"», *Duke Law Journal*, 1991, p. 455. Acerca del mal uso del copyright, véase Mark A. Lemley, «Beyond Preemption: The Law and Policy of Intellectual Property Licensing», *California Law Review*, núm. 87, 1999, p. 111; Mark A. Lemley, «The Economics of Improvement in Intellectual Property Law», *Texas Law Review*, núm. 75, 1997, pp. 989, 1048–1068; en «Intellectual Property and Shrink-wrap Licenses», *Southern California Law Review*, núm. 68, 1995, pp. 1239, 1239, Lemley señala que «los vendedores de software están tratando de "saltarse" masivamente la ley de propiedad intelectual introduciendo en las licencias disposiciones que obligan a sus clientes a adherirse a cláusulas más restrictivas que las que la ley de copyright [...] exigiría». Jessica Litman en «The Tales That Article 2B Tells», *Berkeley Technology Law Journal*, núm. 13, 1998, pp. 931-938, califica de «dudosa» la

enfrentamos en una sociedad de la información —particularmente, los desafíos de carácter político.[72] En otro lugar, identifica nuestra necesidad de un «movimiento ecologista» en el contexto de las políticas de la información —

---

noción de que la ley actual permita a los editores llevar a cabo una operación con una licencia por el mero hecho de designarlo así. A su juicio, el artículo 2B es «confuso y está confundido» acerca del copyright y de su relación con esa ley, dando lugar a una nueva ley. Así, Litman cree que «sea cual sea el resultado» del debate sobre si el copyright tiene sentido en el entorno digital (véase «Reforming Information Law in Copyright's Image», *Dayton Law Review*, núm. 22, 1997, pp. 587, 590), «la doctrina del copyright no está bien adaptada para acomodar muchos de los importantes intereses que conforman nuestras políticas en torno a la información. La Primera Enmienda, la privacidad y los temas de distribución que el copyright ha tratado sólo de pasada son centrales para cualquier política relacionada con la información»; véase también Jessica Litman, «Revising Copyright Law for the Information Age», *Oregon Law Review*, núm. 75, 1996, p. 19 y «The Exclusive Right to Read», *Cardozo Arts and Entertainment Law Journal*, núm. 13, 1994, pp. 29-48, donde Litman declara que «buena parte de la actividad que se desarrolla en la Red tiene lugar sobre el falso supuesto según el cual cualquier material colgado en Internet está libre de copyright a menos que se indique expresamente lo contrario». En «Copyright as Myth», *University of Pittsburgh Law Review*, núm. 53, 1991, pp. 235, 235–37, Litman proporciona una panorámica general sobre las cuestiones de la autoría y de la infracción de la ley de copyright, indicando que este debate continúa girando en torno a la definición de «autoría»; ella habla de «autor» «en el sentido del copyright, de cualquiera que crea obras susceptibles de estar amparadas por la ley de derechos de autor, ya sean libros, canciones, esculturas, edificios, programas informáticos, pinturas o películas» (p. 236, n. 5); también discute por qué la ley de copyright es contraria a la intuición del proceso de autoría. Véase también «The Public Domain», *Emory Law Journal*, núm. 39, 1990, pp. 965-969), donde Litman recomienda una definición amplia del dominio público: «la originalidad es la piedra angular de la ley de copyright» (p. 974). Neil Weinstock Netanel, «Asserting Copyright's Democratic Principles in the Global Arena», *Vanderbilt Law Review*, núm. 51, 1998, pp. 217, n. 48 en p. 232, n. 322 en p. 299; Neil Netanel, «Alienability Restrictions and the Enhancement of Author Autonomy in United States and Continental Copyright Law», *Cardozo Arts and Entertainment Law Journal*, núm. 12, 1994, pp. 1, 42–43; en «[C]opyright and a Democratic Civil Society», *Yale Law Journal*, núm. 106, 1996, pp. 283, 288, 324–336, Netanel analiza la ley y las políticas de copyright en función de su profundización de la democracia: «En esencia, el copyright es una medida del Estado que usa las instituciones del mercado para profundizar en el carácter democrático de la sociedad». Margaret Jane Radin y Polk Wagner, «The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace», *Chicago-Kent Law Review*, núm. 73, 1998; Margaret Jane Radin, *Reinterpreting Property*, Chicago, University of Chicago Press, 1993, pp. 56–63. Pamela Samuelson, «Encoding the Law into Digital Libraries», *Communications of the ACM*, núm. 41, 1999, pp. 13–14; Pamela Samuelson, prólogo a «Symposium: Intellectual Property and Contract Law for the Information Age», *California Law Review*, núm. 87, 1998, p. 1; Pamela Samuelson observa en «Embedding Technical Self-Help in Licensed Software», *Communications of the ACM*, núm. 40, 1997, pp. 13-16, que «quienes colocan bajo licencia software u otra información [...] invocarán generalmente la autoayuda»; véase también la crítica a la «directiva europea sobre bases de datos» en J. H. Reichman y Pamela Samuelson, «Intellectual Property Rights in Data?», *Vanderbilt Law Review*, núm. 50, 1997, pp. 51, 84–95; Samuelson, «The Copyright Grab», *op. cit.*, p. 134; Pamela Samuelson, «Fair Use for Computer Programs and Other Copyrightable Works in Digital Form: The Implications of Sony, Galoob and Sega» *Journal of Intellectual Property Law*, núm. 1, 1993, p. 49.

71 Boyle, *Shamans, Software, and Spleens*, *op. cit.* Para otros relatos categóricos acerca del movimiento general de apropiación privada de la información, véase Debora J. Halbert, *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*, Westport (Conn.), Quorum, 1999.

una retórica que consiga llamar la atención de la gente sobre el amplio abanico de principios que pone en riesgo este movimiento de apropiación de toda la información. La obra de Boyle ha inspirado a muchos otros a lanzar una reivindicación similar de libertad.[73]

Tal libertad limitaría la regulación legal sobre el uso y reelaboración de la cultura y supondría una resistencia al control perfecto sobre aquél, liberando un amplio repertorio de reelaboraciones; construiría mediante protecciones afirmativas la libertad que nos proporcionaba antes el coste del control; y manifestaría lo valioso de esta libertad amparando a las comunidades que ésta propicie.

Ahora bien, esta libertad podría construirse mediante cambios legales y también de forma voluntaria. Es decir, podría restablecerse un equilibrio legal que promoviera ciertas libertades consideradas importantes, o bien podría manejarse la propiedad de otro modo que permitiese ejercer esas mismas libertades.

Esta segunda estrategia fue la técnica empleada por el movimiento de *software libre*, descrito en el Capítulo 8. Valiéndose de la ley de copyright, Stallman concibió una licencia de software que garantizaba las cuatro libertades del *software libre*, al tiempo que obligaba a quienes lo modificaban y distribuían a hacerlo de forma libre. Así pues, esta licencia creó un procomún de software, dado que éste está disponible para que cualquiera pueda usarlo; dicho procomún se ha convertido en una materia prima crucial que estimula singularmente la era digital.

Seth Shulman confiere a esta historia un toque dramático muy adecuado en *Owning the Future*, Boston, Houghton Mifflin, 1999. Para la edición a través de Internet y la propiedad intelectual, véase Brian Kahin y Hal R. Varian (eds.), *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*, Cambridge (Mass.), MIT Press, 2000. Sobre propiedad intelectual y propiedad intangible, Adam Jolly y Jeremy Philpott (eds.), *A Handbook of Intellectual Property Management: Protecting, Developing and Exploiting Your IP Assets*, Londres, Kogan Page, 2004.

72 «Somos partidarios de un desplazamiento del enfoque centrado en el autor en dos direcciones; primero, hacia el reconocimiento de un número limitado de nuevas protecciones relacionadas con la herencia cultural, las producciones folclóricas y los conocimientos prácticos de naturaleza biológica. Y segundo, somos partidarios de forma general de incrementar el reconocimiento y la protección del dominio público por medio de "protecciones del uso justo" amplias, de licencias obligatorias y, en primer lugar, de una cobertura inicial más estrecha de los derechos de propiedad»; Boyle, *Shamans, Software, and Spleens*, *op. cit.*, p. 169.

73 James Boyle, «A Politics of Intellectual Property: Environmentalism for the Net?», *Duke Law Journal*, núm. 47, 1997, p. 87.

Más recientemente la idea de Stallman ha sido copiada por otras personas que tratan de reconstruir un procomún en el ciberespacio. El proyecto de la Wikipedia, por ejemplo, ha generado —ante el asombro de la mayoría— una extraordinaria enciclopedia *online* exclusivamente mediante el esfuerzo colectivo de miles de voluntarios, que aportan sus artículos y revisiones a través de un *wiki* público. El fruto de este trabajo está ahora protegido para siempre (sí, ya sé, sólo durante un «tiempo limitado», pero no me corrija el lector por ese pequeño detalle) mediante una licencia copyright que, como la GPL, exige que cualquier modificación se distribuya a su vez de forma igualmente libre. (Más sobre la Wikipedia en el Capítulo 12).

Y, del mismo modo, Creative Commons también ha usado la ley privada para erigir un procomún público de carácter efectivo. Insisto, siguiendo el ejemplo de Stallman, Creative Commons ofrece a los titulares del copyright una manera sencilla de marcar su obra creativa con las libertades que decidan. Esta marca es una licencia que reserva algunos derechos al autor, al tiempo que cede otros al público que, de otra forma, estarían restringidos de forma privada. Y como estas licencias son públicas y no exclusivas, también contribuyen en la práctica a generar un procomún de materiales creativos al que cualquiera puede recurrir para producir sucesivas obras.

Aunque he dedicado una gran cantidad de mi tiempo a colaborar en la construcción de Creative Commons, creo sin embargo que la acción privada no basta por sí sola. No obstante, podemos aprender algo muy valioso de lo que dicha acción privada produce, ya que esta lección puede contribuir a que, en el futuro, los legisladores recompongan las leyes de copyright.

11. Privacidad

La conclusión de la Primera Parte fue que el código podía permitir un ciberespacio más regulable; la conclusión de la Segunda Parte fue que el código se erigiría en un regulador cada vez más importante en ese espacio más regulable. Ambas conclusiones fueron centrales en la historia del capítulo anterior. En contra del prematuro pánico de los titulares de derechos de autor, Internet se convertirá en un espacio donde la propiedad intelectual podrá protegerse más fácilmente. Como he descrito, tal protección se efectuará a través del código.

La historia de la privacidad es sorprendentemente similar. Es más, como Jonathan Zittrain expuso en un ensayo publicado en la revista *Stanford Law Review,*[1] los problemas de la privacidad y del copyright son exactamente los mismos. En ambos hay una parte de «nuestros» datos sobre la que «hemos» perdido el control. En el caso del copyright, se trata de datos que constituyen una copia de nuestra obra sujeta a derechos de autor; en el caso de la privacidad, se trata de datos que presentan algún hecho sobre nosotros. En ambos casos, esta pérdida de control la ha provocado Internet: con el copyright, porque la tecnología posibilita copias perfectas y gratuitas del contenido; con la privacidad, como veremos en este capítulo, porque la tecnología posibilita un control de la conducta permanente y barato. En ambos casos, la pregunta que deberían plantearse los legisladores es qué combinación de ley y tecnología podría restaurar el nivel adecuado de control. Este nivel debe equilibrar los intereses privados y los públicos: en el capítulo anterior describí tal equilibrio con respecto al copyright; en éste, exploraré este equilibrio con respecto a la privacidad.

---

1 Véase Jonathan Zittrain, «What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication», *Stanford Law Review*, núm. 52, 2000, p. 1201.

La gran diferencia entre el copyright y la privacidad, no obstante, es la política económica que busca una solución para cada problema. Con el copyright, los intereses amenazados son poderosos y están bien organizados; con la privacidad, los intereses amenazados son difusos y están desorganizados. Con el copyright, los principios situados al otro lado de la protección (el procomún o el dominio público) ni son imperiosos ni son bien comprendidos. Con la privacidad, los principios situados en el otro lado de la protección (la seguridad, la guerra contra el terrorismo) son imperiosos y han sido bien comprendidos. El resultado de estas diferencias, como cualquier teórico político pronosticaría, es que en los últimos diez años, al tiempo que veíamos numerosas modificaciones legislativas y técnicas para resolver los problemas relativos a los derechos de autor, hemos visto muy pocas que resuelvan los problemas de la privacidad.

Ahora bien, al igual que con el copyright, podríamos reencontrar el equilibrio que proteja la privacidad. Hay modificaciones tanto legales como tecnológicas que podrían producir un entorno digital mucho más privado (y seguro). El hecho de que las llevemos a cabo o no dependerá de que reconozcamos tanto la dinámica de regulación en el ciberespacio como la importancia del principio de privacidad.

A continuación, reflexionaremos sobre tres aspectos de la privacidad, y sobre cómo el ciberespacio ha cambiado cada uno de ellos. En este capítulo nos centraremos en dos de esos aspectos, si bien empezaré por el tercero para ayudar a orientar el equilibrio.

Privacidad en privado

El problema tradicional en relación con la «privacidad» se centraba en el límite que establecía la ley sobre la capacidad de otros para entrar en el espacio privado de cada uno. ¿Qué derecho tiene el Estado a entrar en nuestra casa, o a registrar nuestros papeles? ¿Qué protección nos otorga la ley de allanamiento si otras instancias distintas al Estado fisgonean en nuestros asuntos privados? He aquí uno de los significados del lema de Brandeis, «el derecho a ser dejado en paz».[2] Desde la perspectiva legal, la privacidad es el conjunto de restricciones legales sobre el poder de los demás para invadir un espacio protegido.

2 *Olmstead vs. United States*, 277 US 438, 1928.

Tales restricciones legales fueron complementadas con barreras físicas. Por más que la ley de allanamiento diga que es ilegal entrar en mi casa de noche, ello no implica que no echemos el cerrojo de nuestras puertas y ventanas. También en este caso, la protección de la que disfrutamos es la suma de las protecciones proporcionadas por las cuatro modalidades de regulación. La ley complementa las protecciones tecnológicas, las incorporadas en las normas y las derivadas del alto coste del allanamiento ilegal.

Las tecnologías digitales han variado estas protecciones. El precio de la tecnología de los micrófonos parabólicos ha disminuido drásticamente, con lo que me resulta más fácil escuchar lo que dice el lector a través de su ventana. Por otra parte, el coste de las tecnologías de seguridad para controlar las intrusiones ha disminuido en la misma medida. El saldo final de tales cambios es difícil de calcular, pero esta dificultad no vuelve ambiguo el principio fundamental. Las nuevas tecnologías no cuestionan la expectativa de privacidad en lo que se entiende razonablemente como espacios «privados», por lo que esta clase de privacidad no presenta una «ambigüedad latente».

Privacidad en público: vigilancia

Hay un segundo tipo de privacidad que a primera vista parece un oxímoron —la privacidad en público. ¿Qué clase de protección existe contra la recopilación de información sobre mi persona cuando estoy en un espacio público o embarco en un avión?

La respuesta tradicional era simple: ninguna. Al mostrarnos en público, renunciábamos a todo derecho a ocultar o controlar lo que los demás llegasen a saber sobre nosotros. Los hechos que transmitíamos acerca de nosotros mismos eran «libres como el aire para el uso común».[3] La ley no proporcionaba protección legal contra el uso de la información recabada en contextos públicos.

Pero como hemos visto una y otra vez, el simple hecho de que la ley de privacidad no nos protegiese no significaba que no estuviéramos protegidos. Los hechos acerca de nosotros que transmitimos cuando estamos en

3 *International News Service vs. Associated Press*, 248 U.S. 215, 250, 1918 (voto particular del juez Brandeis).

público, pese a no estar legalmente protegidos, lo están en la práctica por el alto coste que conlleva su recopilación y su uso. Esta dificultad se convierte así en el mejor amigo de la privacidad.

Sin embargo, para ver la protección que esto supone, debemos distinguir entre dos dimensiones en las que la privacidad podría verse comprometida.

Hay una parte de la vida de cualquiera de nosotros que está controlada, y hay una parte que puede ser registrada. La primera es esa parte de nuestra existencia cotidiana que los demás ven o advierten y a la que pueden responder, siempre que la respuesta sea adecuada. Al andar por la calle, mi conducta es controlada. Si caminase por la calle de un pueblecito de China occidental, dicha conducta sería supervisada de forma bastante exhaustiva. En ambos casos, este control sería transitorio. La gente se fijaría en mí, por ejemplo, si andara con un elefante o llevase un vestido, pero si no hubiera nada especial en mi caminar, si simplemente me mezclase entre la multitud, entonces podría ser advertido durante un instante y olvidado poco después —quizá con más rapidez en San Francisco que en China.

En cuanto a la registrable, es la parte de nuestra vida que deja, o constituye, un indicio. Los garabatos de nuestro diario son un registro de nuestros pensamientos. Las cosas de nuestra casa son un registro de lo que poseemos. Las grabaciones de nuestro contestador son un registro de quién nos llamó y qué nos dijo. Nuestro disco duro *somos* nosotros. Estas partes de nuestra vida no son efímeras, sino que perduran para ser revisadas —al menos si la tecnología y la ley lo permiten.

Estas dos dimensiones pueden interactuar, dependiendo de la tecnología de cada una de ellas. En un pueblo pequeño cada uno de mis movimientos puede ser controlado por mis vecinos, lo cual produce un registro —en sus memorias. Ahora bien, dada la naturaleza de esta *tecnología*, al Estado le resulta bastante costoso acceder a dicho registro. Los agentes de policía tienen que interrogar a los vecinos y después triangular los relatos de éstos inevitablemente incompletos para discernir qué partes son verdad y qué partes no. Se trata de un procedimiento conocido, pero que tiene sus límites. Podría ser fácil interrogar a los vecinos para reunir información que ayudase a localizar a una persona perdida, pero si el Estado les preguntara acerca de las opiniones políticas de un vecino, podríamos esperar (¿desear?) que se resistieran a responder. Por lo tanto, en principio la información estaría ahí, si bien en la práctica resultaría costoso extraerla.

Las tecnologías digitales varían este equilibrio —radicalmente. Y es que no sólo determinan que haya más conductas controlables, sino también que haya más conductas registrables. Las mismas tecnologías que recopilan datos ahora lo hacen de un modo que permite rastrearlos. Así pues, la vida se convierte cada vez más en un pueblo compuesto de procesadores paralelos, accesibles en cualquier momento para reconstruir acontecimientos o seguirle la pista a determinadas conductas.

Contemplemos algunos ejemplos familiares:

Internet

En la Primera Parte, describí el anonimato que proveía originalmente Internet, pero tengamos claro algo importante: aquel relativo anonimato de los «viejos tiempos» actualmente ha desaparecido en la práctica. Dondequiera que naveguemos en Internet, queda registrado que la dirección IP xxx.xxx.xxx.xxx estuvo allí. Dondequiera que naveguemos y hayamos permitido que almacenen una *cookie* en nuestro disco duro, queda registrado que el ordenador con dicha *cookie* estuvo allí —así como los datos asociados con ella. Se nos conoce por nuestros clics de ratón. Y a medida que los negocios y los publicistas colaboran más estrechamente, la cantidad de información que se puede acumular sobre nosotros se vuelve infinita.

Consideremos una hipótesis que es completamente posible desde un punto de vista técnico, dada la arquitectura existente de la Red: el lector accede a la página web de una compañía en la que confía y le facilita todos y cada uno de sus datos privados —nombre, dirección, número de la Seguridad Social, revistas y programas de televisión favoritos, etc. Esta compañía deposita una *cookie* en el ordenador del lector. Éste accede a continuación a otro sitio, uno en el que no confía, y decide no facilitarle ninguna información personal. Ahora bien, el lector no tiene modo de saber si estas compañías están compartiendo los datos que cada una de ellas recopila. Es perfectamente posible que sincronicen los datos de las *cookies* que crean y, por consiguiente, no existe ninguna razón técnica por la que, una vez que el lector facilita sus datos en una primera ocasión, éstos no puedan ser conocidos por un amplio abanico de sitios a los que acceda después.

En la siguiente sección, consideraremos más exhaustivamente cómo deberíamos pensar sobre la privacidad de cualquier dato que hayamos proporcionado a otros, como nuestro nombre, dirección o número de la Seguridad Social. Por el momento, sin embargo, centrémonos en los datos de identificación recopilados mientras nos movemos en «público». A no ser que hayamos tomado medidas extraordinarias —instalando software de privacidad en nuestro ordenador, bloqueando las *cookies*, etc. — no hay razón para pensar que nadie podrá saber que visitamos ciertas páginas o hicimos ciertas búsquedas. De hecho, esa información se puede conocer perfectamente. Las capas de tecnología diseñadas para identificar «al cliente» han producido interminables capas de datos que pueden conducirlos hasta nosotros.

Búsquedas

En enero de 2006, Google sorprendió al gobierno estadounidense haciendo lo que ninguna otra compañía de búsquedas había hecho antes: decirle que «no». El Departamento de Justicia había iniciado un estudio sobre pornografía en la Red para apoyar la última regulación del Congreso al respecto. Así pues, quería información sobre la frecuencia y la forma en que la gente busca pornografía en Internet, y le pidió a Google que le proporcionase un millón de búsquedas aleatorias de su base de datos a lo largo de un periodo concreto. Google —a diferencia de Yahoo! y MSN— se negó.

Sospecho que, al oír esto por primera vez, la mayoría de la gente se hizo una pregunta obvia —¿Google conserva datos sobre las solicitudes de búsqueda? En efecto. La curiosidad está bajo control, produciendo una base de datos de curiosos que puede ser consultada. Para averiguar cómo hacer mejor su trabajo, Google —y todos los demás motores de búsqueda—[4] conserva una copia de todas las búsquedas que le solicitan. Y lo que es más inquietante, Google asocia esa búsqueda a una dirección IP específica y, si es posible, a una cuenta de usuario de Google. Por consiguiente, en las entrañas de la base de datos de Google, hay una lista de todas las búsquedas que hemos realizado cuando estábamos registrados en nuestra cuenta de Gmail, una lista que está ahí, esperando que alguien pida verla.

---

4 Declan MCullagh y Elinor Mills recopilaron las prácticas de todos los principales motores de búsqueda en «Verbatim: Search Firms Surveyed on Privacy», *CNET NEWS*, 3 de febrero de 2006, disponible en http://news.com.com/2100-1025_3-6034626.html.

Y el gobierno estadounidense lo pidió. En el curso normal de los acontecimientos, tal requerimiento gubernamental resultaría completamente ordinario. No se discute que el gobierno pida a quienes poseen pruebas relevantes que las proporcionen para una investigación abierta de índole civil o criminal (existen límites, pero ninguno realmente significativo). Google posee pruebas y el gobierno, de manera habitual, tendría derecho a acceder a ellas.

Además, en este caso, el gobierno prometió explícitamente que sólo usaría dichas pruebas para evaluar las pautas de consumo relativas a la pornografía. En concreto, prometió que no rastrearía ninguna búsqueda particularmente sospechosa, ignorando estas pruebas —que normalmente podría usar libremente para cualquier propósito— con tal de tener acceso al conjunto de datos acerca de las búsquedas de pornografía.

Así pues, ¿cuál es el problema que ilustra este ejemplo?

Antes de que surgieran los motores de búsqueda, nadie poseía registros de la curiosidad; no había ninguna lista de las preguntas que se formulaban. Ahora sí. La gente inunda obsesivamente los motores de búsqueda con preguntas sobre cualquier cosa. La inmensa mayoría de ellas es totalmente inofensiva («setas Y *ragoût*»), si bien algunas muestran rasgos no tan inofensivos de quienes buscan («fotografías eróticas Y niños»). Ahora existe una lista de todas estas preguntas, algunas de las cuales proporcionan pruebas de, como mínimo, propósitos criminales.

El interés del gobierno en esta lista aumentará con el tiempo. Al principio sus demandas parecerán bastante inocuas —¿qué hay de malo en que cuente el número de veces que la gente pide a Google que le indique dónde encontrar fotografías eróticas? A partir de aquí, las demandas se vincularán a conductas muy dañinas —búsquedas que sugieran terrorismo o abusos. ¿Quién podría impugnar tal revelación? Finalmente cuando las demandas no sean tan inocuas, ni los crímenes a las que se vinculen tan perniciosos, simplemente se insistirá en que se trata de un modo eficaz de hacer cumplir la ley. «Si no te gusta la ley, cámbiala. Pero hasta que lo hagas, permítenos velar por su cumplimiento». La progresión es obvia, inevitable e irresistible.

Correo electrónico

El correo electrónico es un mensaje basado en texto que se almacena de forma digital. Es como la trascripción de una llamada telefónica. Cuando una persona se lo envía a otra, el correo electrónico se copia y se transmite de máquina a máquina, permaneciendo en ellas hasta que es eliminado, bien mediante rutinas —decisiones de las máquinas—, bien mediante la decisión de los usuarios.

El contenido de muchos mensajes de correo electrónico es como el de una llamada telefónica ordinaria —carente de planificación y reflexión, la típica cháchara de amigos. Ahora bien, a diferencia de una llamada telefónica, éste contenido es archivado en una forma registrable. En la actualidad las compañías invierten millones en tecnologías que exploran las conversaciones de los empleados, conversaciones que antes eran completamente privadas. Tanto en tiempo real como de forma retrospectiva, el contenido de las conversaciones puede llegar a conocerse. Sobre la base teórica de que «los ordenadores les pertenecen»,[5] los jefes fisgonean cada vez más en el correo electrónico de sus empleados en busca de materiales que estimen inadecuados.[6]

En principio es posible realizar este control y registro con las llamadas de teléfono o con las cartas. En la práctica estas comunicaciones no están bajo control, puesto que se requiere tiempo y dinero —es decir, intervención humana. Y este coste implica que la mayoría se niegue a controlarlas, con lo que, una vez más, vemos que el coste del control concede un cierto tipo de libertad.

Controlar a los empleados (o a los cónyuges) es un nuevo uso muy importante de las tecnologías de correo electrónico, y también lo es mejorar el envío de publicidad. Google es de nuevo el líder en esto, con su nuevo servicio Gmail. Gmail puede mostrarnos publicidad mientras leemos nuestro correo electrónico, pero el gran avance es que el anuncio se genera en función del contenido del correo electrónico. Imagínese el lector una televisión

---

5 Stefik, *The Internet Edge*, *op. cit.*, p. 20.

6 El Estado también puede fisgonear los correos electrónicos, pero sólo si cuenta con una orden. Normalmente se requiere que avise, pero el Estado puede conseguir una prórroga de noventa días para proporcionar tal aviso. Véase US Code Title 18, Section 2705(a)(i).

que variara los anuncios al oír su conversación telefónica. El contenido del correo electrónico —y quizás el contenido de nuestra bandeja de entrada en general— ayuda a determinar qué es lo que se nos muestra.

Para hacer que este sistema funcione bien, Google necesita que conservemos un montón de datos en sus servidores, de modo que lo único difícil de hacer en Gmail —y es realmente dificilísimo— es eliminar el contenido de una cuenta de Google Gmail. Gmail permite eliminar las pantallas de una en una, pero cuando tenemos 20.000 mensajes en la bandeja de entrada, ¿quién tiene tiempo de eliminarlos? ¿Le costaría mucho a Gmail habilitar la función «Eliminar todo»? Por supuesto que no. ¡Estamos hablando de Google! De esta forma, mediante un uso inteligente de la arquitectura, Google se asegura de que se conservan más datos, y de que éstos se convierten luego en un recurso para otros fines. Si el lector se viese alguna vez involucrado en un juicio, la primera pregunta del abogado de la parte contraria debería ser —¿tiene usted una cuenta de Gmail? Porque si es así, la vida del lector estará expuesta a revisión.

Correo de voz

Si el correo electrónico se convierte en un registro permanente, ¿por qué no el correo de voz? Los sistemas de correo de voz archivan los mensajes y registran los atributos de las conversaciones. A medida que mejoran las tecnologías de reconocimiento de voz, también lo hace la capacidad de analizar los registros de voz. A medida que los sistemas de correo de voz se hacen digitales, archivando el contenido en servidores centrales en lugar de en dispositivos de 50 dólares conectados al teléfono doméstico, se convierten en recursos de registro muy prácticos. En principio, el Estado podría supervisar cada noche todas las grabaciones de voz almacenadas por todas las compañías telefónicas del país. Este registro no supondría ninguna carga para el usuario: podría dirigirse y limitarse a temas específicos, y podría operar en segundo plano sin que nadie lo supiera jamás.

Voz

¿Y por qué detenerse en las grabaciones? Según un informe, la NSA controla más de 650 millones de conversaciones telefónicas *al día*,[7] y esto de forma automática. Este control solía restringirse a los extranjeros, pero por lo que parece, ahora el sistema controla una gama extraordinaria de comunicaciones en busca de ese dato o esa pista que despierte la sospecha investigadora. El sistema produce algo semejante a un informe del tiempo, así como unos indicadores particularizados. Existen, por ejemplo, mediciones de «cháchara» que pueden indicar la llegada de una tormenta.

Este control, como cada uno de los ejemplos anteriores, no supone carga alguna para quienes usan el teléfono, que no saben que algo les está escuchando al otro extremo de la línea. El sistema trabaja silenciosamente en segundo plano, registrando esta comunicación controlada en tiempo real.

Vídeo

En cada uno de los ejemplos descritos hasta el momento, alguien elige usar una tecnología que hace vulnerable su privacidad. El cambio se produce cuando esa tecnología evoluciona para simplificar el control y el registro de conductas.

Ahora bien, esa misma evolución se está dando también fuera de la Red. De hecho, se está dando en el espacio público por excelencia —las calles o los lugares de reunión pública. Este control es el producto de la actual versión de la tecnología de vídeo. Originalmente, las cámaras de vídeo suponían una forma relativamente benigna de vigilancia. Dado que el resultado de su control dependía únicamente de la interpretación humana, había relativamente pocos contextos en los que mereciera la pena tener a alguien vigilando las grabaciones. Y si nadie las vigilaba, el uso de estas tecnologías se limitaba a

---

7 Véase Richard Posner, «Our Domestic Intelligence Crisis», *Washington Post*, 21 de diciembre de 2005, disponible en http://www.washingtonpost.com/wp-dyn/content/discussion/2005/12/20/DI2005122001142.html.

rastrear las conductas negativas después de que se produjeran. A pocos parece molestarles que la cámara de vídeo de un supermercado permita identificar al criminal que ha asesinado al dependiente.

En cualquier caso, la tecnología digital ha cambiado el vídeo, que ahora es una herramienta de inteligencia, y no simplemente de grabación. En Londres, como he descrito, hay cámaras repartidas por todo el distrito central para controlar qué coches entran en él, de modo que los no residentes deben pagar un impuesto especial para circular por «zonas de congestión». Las cámaras graban e interpretan las matrículas, y a continuación determinan si esos coches pagaron el impuesto correspondiente. El objetivo del sistema era minimizar la congestión de tráfico en Londres, y su consecuencia es la creación de una base de datos de cada coche que entra en Londres, vinculado a una hora y un lugar concretos.

Pero el uso más ambicioso de la vídeovigilancia es el reconocimiento del rostro humano. Por más que la tecnología tuviera muy mala prensa cuando se introdujo por primera vez en Tampa,[8] el Estado continúa fomentando que las compañías desarrollen la capacidad de identificar quién es alguien mientras éste se halla en un lugar tradicionalmente anónimo. Como anuncia un vendedor, «la tecnología de reconocimiento facial es la tecnología biométrica menos intrusiva y más rápida. [...] No hay intrusión ni demora, y los sujetos son completamente inconscientes del proceso en la mayoría de los casos. No sienten que están "bajo vigilancia" ni que su privacidad ha sido invadida».[9]

Estas tecnologías no son aún fiables, pero siguen recibiendo financiación tanto de inversores privados como del gobierno. Éste, de hecho, lleva a cabo pruebas bianuales para estimar la fiabilidad de dichas tecnologías.[10] Debe de haber al menos alguien que espere que algún día sea posible emplear una cámara para identificar quién está entre la multitud, o quién se subió a un tren.

---

8 Véase, por ejemplo, L. Grossman, «Welcome to the Snooper Bowl», *Time*, 12 de febrero de 2001, disponible en http://www.time.com/time/archive/preview/0,10987,999210,00.html; D. McCullagh, «Call It Super Bowl Face Scan I», *Wired*, 2 de febrero de 2001, disponible en http://www.wired.com/news/politics/0,1283,41571,00.html.

9 C-VIS, «What is Face Recognition Technology?», disponible en http://www.c-vis.com/ htd/frt.html. Para una argumentación que defiende que el reconocimiento facial debería considerarse una violación de la Cuarta Enmienda, véase Alexander T. Nguyen, «Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked The Fourth Amendment?», *Virginia Journal of Law and Technology*, núm. 7, 2002, p. 2.

10 Véase la página principal de *Face Recognition Vendor Test*, (Test del vendedor de reconocimiento facial) disponible en http://www.frvt.org.

Partes del cuerpo

Los criminales dejan tras de sí pruebas, tanto porque no suelen ser excesivamente racionales como porque resulta muy difícil no hacerlo. Pues bien, la tecnología está poniéndoselo aún más complicado. Con la tecnología del ADN, los criminales lo tienen cada vez más difícil para evitar dejar su marca, y las autoridades cada vez más fácil para identificar con una fiabilidad extremadamente alta si X hizo Y.

Algunas naciones han comenzado a sacar provecho de esta nueva ventaja. Y, una vez más, Gran Bretaña va en cabeza.[11] A comienzos de 1995, el gobierno británico empezó a recopilar muestras de ADN para incluirlas en un registro nacional. El programa se promovió, en un principio, como una manera de luchar contra el terrorismo, pero en una década su uso se ha vuelto mucho más indiscriminado.

En diciembre de 2005, mientras viajaba en el transporte público londinense, leí lo siguiente en un anuncio público:

> Abusos, agresiones, arrestos: nuestro personal está aquí para ayudarle. Escupir al personal del DLR [*Docklands Light Railway*, tren ligero de Docklands] se considera una agresión y constituye un delito. Los «equipos de recuperación de saliva» están disponibles en todos los trenes y se usarán para identificar a los infractores en la base de datos nacional de ADN.

¿Por qué no? Puede que escupir sea inofensivo, pero es insultante. Así pues, si existen herramientas para identificar al autor del insulto, ¿por qué no usarlas?

En todos estos casos, tecnologías diseñadas sin tener como fin el control, o sólo con una capacidad limitada de control, se han convertido ahora en tecnologías especializadas para llevarlo a cabo. La combinación de estas tecnologías produce una gama extraordinaria de datos registrables. Y lo que es más importante, a medida que maduren dichas tecnologías, nadie que viva en el seno de la sociedad ordinaria dispondrá, en esencia, de ningún modo de escapar a esta supervisión. Así, el control para producir datos registrables

---

11 Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, Nueva York, Random House, 2004, pp. 34–53.

se convertirá en la arquitectura del espacio público por defecto, algo tan normalizado como la iluminación de las calles. Desde la simple capacidad de seguirle la pista a un individuo hasta la más inquietante de saber qué quiere o qué hace en cualquier momento, esta perfeccionada infraestructura de datos produce un panóptico que supera cualquier cosa que Bentham pudiera haber imaginado.[12]

«Orwell» es la palabra que el lector está buscando en este momento. Y por más que esté convencido de que las analogías orwellianas son casi siempre inútiles, introduzcamos aquí una pese a todo. Aunque los objetivos del gobierno en *1984* eran de largo más malvados que cualquiera que pudiera perseguir nuestro gobierno, resulta interesante apuntar cuán ineficaces eran las tecnologías orwellianas con respecto a la gama actual de tecnologías. El dispositivo fundamental era una «pantalla de televisión» que emitía contenidos al tiempo que controlaba la conducta de quienes se hallaban al otro lado. Ahora bien, la gran ventaja de la pantalla de televisión era que uno conocía, en principio, lo que ésta podía ver. Así, Winston sabía dónde esconderse porque la perspectiva de la pantalla era transparente.[13] Por consiguiente, al ser fácil saber lo que la pantalla no podía ver, también lo era saber dónde hacer aquello que uno no quería que ésta viese.

Ése no es el mundo en que nosotros vivimos hoy: no podemos saber si lo que buscamos en Internet está siendo controlado; tampoco si una cámara está intentando identificar quiénes somos; nuestros teléfonos no hacen ya divertidos chasquidos cuando la NSA los pincha; nuestro correo electrónico no nos informa cuando algún programa espía lo ha fisgoneado. Las tecnologías de hoy no tienen nada de la integridad de las de *1984*. Ninguna tecnología actual es lo bastante decente como para avisarnos cuando nuestra vida está siendo grabada.

---

12 Jeremy Bentham (1748-1832), filósofo inglés considerado el padre del utilitarismo, en 1791 propuso un diseño innovador de prisión al que denominó «Panóptico». El modelo penitenciario de Bentham consistía en un edificio anular dividido en celdas individuales sin conexión visual entre ellas, pero equipadas con dos ventanas, una de las cuales daba a una garita central desde la que era posible observar a todos los presos sin que éstos supieran cuándo estaban siendo vigilados. De este modo, no sólo se reducían los costes de personal y se permitía la discontinuidad de la vigilancia, sino que, virtualmente, los presos podrían acabar por no necesitar ser custodiados porque habrían interiorizado el control hasta el punto de vigilarse a sí mismos. [N. del E.]

13 Lawrence Lessig, «On the Internet and the Benign Invasions of Nineteen Eighty-Four», en Abbott Gleason, Jack Goldsmith y Martha C. Nussbaum (eds.), *On «Nineteen Eighty-Four»: Orwell and Our Future*, Princeton, Princeton University Press, 2005, p. 212.

Existe, asimismo, una segunda diferencia. El gran fallo del diseño de *1984* radicaba en cómo se imaginaba que se controlaría la conducta. En la historia no había ordenadores, sino que el control era ejercido por una cuadrilla de guardias que observaba varios monitores de televisión. Ahora bien, tal control no posibilitaba que los guardias pudieran conectar sus respectivas inteligencias. No existía un sistema de búsqueda a través de los cerebros de los guardias. Por supuesto, un guardia podía observar que alguien estaba hablando con quien no debía, o que había entrado en una parte de la ciudad donde no debería estar. Pero ningún guardia disponía individualmente de una panorámica completa de la vida de Winston.

Una vez más, esa «imperfección» puede ahora quedar eliminada, ya que podemos controlar todo y consultar el resultado de dicho control. Ni el propio Orwell pudo imaginar algo así.

Hasta el momento he examinado un abanico de diversas tecnologías para identificar una forma común. En todas ellas el individuo actúa en un contexto técnicamente público, si bien no estoy afirmando que dicho contexto debiera ser tratado legalmente como «público», en el sentido de que la privacidad no deba protegerse. Por ahora dejo de lado esa cuestión. Lo que quiero destacar es que el individuo expone sus palabras o sus imágenes en un contexto que no controla. Un paseo por la Quinta Avenida de Nueva York es el ejemplo más claro de ello; otro es el envío de una carta. En ambos casos, el individuo se sumerge en un flujo de actividad que escapa de su control.

Así pues, el interrogante que se nos plantea es qué límites debería haber —en nombre de la privacidad— a la capacidad de vigilar estas actividades. Pero incluso ese interrogante describe la cuestión de forma demasiado amplia. Cuando hablo de «vigilar» no me refiero a la vigilancia en general, sino justamente a la forma específica de vigilancia que los ejemplos anteriores ponen de manifiesto. Es decir, me refiero a lo que podríamos denominar «vigilancia digital».

Esta «vigilancia digital» es el proceso por el que cierta forma de actividad humana es analizada por un ordenador de acuerdo con alguna norma específica. Dicha norma podría ser «marcar todos los correos electrónicos que hablen de Al Qaeda», o bien «marcar todos los correos electrónicos que elogien al gobernador Dean». Insisto en que en este momento no abordo la cuestión normativa o legal de si tal vigilancia debiera permitirse, sino que me limito a una tarea definitoria. En cada uno de los casos mencionados, el rasgo crucial es que un ordenador está clasificando datos para su subsiguiente revisión por humanos. La sofisticación de la búsqueda es una cuestión técnica, pero no cabe duda de que su precisión está mejorando sustancialmente.

Así pues, ¿debería permitirse esta forma de control?

Cuando planteo esta pregunta en estos precisos términos, me suelo encontrar con dos reacciones antagónicas. En un extremo, los amantes de la privacidad defienden que no hay nada nuevo en la vigilancia digital. Según ellos, no hay diferencia entre que la policía lea el correo postal del lector y que el ordenador de la policía lea su correo electrónico. En ambos casos se ha infringido una expectativa de privacidad legítima y razonable, y en ambos casos la ley debería proteger al lector ante tal infracción.

En el otro extremo, los amantes de la seguridad insisten en que hay una diferencia fundamental en lo que respecta a la vigilancia digital. Tal y como escribió el juez Richard Posner en el *Washington Post*, en un artículo donde defendía la (exhaustiva)[14] vigilancia de las comunicaciones nacionales implantada por la administración Bush, «la recopilación y el tratamiento

---

14 Los estadounidenses hemos sabido de la profunda implicación del Departamento de Defensa de EEUU en el espionaje nacional (espionaje relacionado con amenazas a la seguridad nacional radicadas en territorio estadounidense). En este sentido, la Agencia de Seguridad Nacional (NSA) ha estado realizando, fuera del ámbito legal establecido en la FISA (*Foreign Intelligence Surveillance Act*, Ley de Vigilancia de Espionaje Exterior), una vigilancia electrónica de ciudadanos estadounidenses dentro del país. Otras agencias del Pentágono, especialmente la conocida como CIFA (*Counterintelligence Field Activity*, Actividad de Contraespionaje), han estado implicadas en espionaje nacional a gran escala, según describe Walter Pincus en una serie de artículos publicados en el *Washington Post* a finales de 2005. Aunque la misión formal de la CIFA es evitar ataques contra instalaciones militares en EEUU, la magnitud de sus actividades invita a una preocupación más amplia con respecto a la seguridad nacional. Otras agencias del Pentágono también se han involucrado en tareas de espionaje nacional, como el IDC (*Information Dominance Center*, Centro de Control de la Información), que desarrolló el programa de extracción de información *Able Danger*. Richard Posner, «Our Domestic Intelligence Crisis», *Washington Post*, 21 de diciembre de 2005, en A31.

[El 9 de julio de 2008 el Senado de EEUU, de mayoría demócrata, aprobó por amplia mayoría el proyecto de reforma de la FISA (cuyo texto anterior databa de 1978). Dicha reforma supone dotar de amparo legal a la política indiscriminada de espionaje de llamadas telefónicas (incluidas las realizadas mediante teléfono móvil) y correos electrónicos impulsada por la administración Bush a partir del 11-S, amén de conceder inmunidad retroactiva a las empresas de telecomunicaciones que desde entonces colaboran con el gobierno estadounidense en dichas tareas (y que se enfrentaban a varias decenas de demandas multimillonarias por violación de la Cuarta Enmienda). Pese a aseverar en un comunicado oficial del 17 de diciembre del 2007 que «conceder tal inmunidad socavaría las protecciones constitucionales que los estadounidenses confían serán protegidas por el Congreso» y que, por lo tanto, apoyaría «la obstrucción de este proyecto de ley», el entonces candidato presidencial Barack Obama fue uno de los 69 senadores que votaron a favor de la ley, lo cual provocó una gran indignación entre sus simpatizantes en plena precampaña electoral. El propio Lawrence Lessig (víctima también de la «histeria ante la inmunidad») ha seguido activa y puntualmente esta polémica desde su *blog*: http://lessig.org/blog. (N. del E.)]

mecánicos de información no pueden, como tales, invadir la privacidad». ¿Por qué? Porque el tratamiento de la información lo lleva a cabo una máquina. Y las máquinas no cotillean, ni se inmiscuyen en la aventura que alguien tiene con su colega de trabajo, ni tampoco le castigan por sus opiniones políticas. Se trata simplemente de máquinas lógicas que actúan en función de una serie de condiciones. Es más, como sostiene Richard Posner, «su criba inicial, lejos de invadir la privacidad (un ordenador no es un ser sensible), mantiene la mayoría de la información privada a salvo de ser leída por cualquier oficial de espionaje». Es mucho mejor que sean máquinas las que lean nuestro correo electrónico, sugiere Posner, tanto por el aumento de seguridad que ello conlleva como porque el fisgón alternativo —un oficial de espionaje— sería mucho más indiscreto.

Ahora bien, sugerir que este sistema está exento de costes sería ir demasiado lejos. Si viviéramos en un mundo donde todas y cada una de nuestras comunicaciones estuvieran bajo control (¿si viviéramos?), eso modificaría ciertamente el sentido de aquel derecho a «ser dejado en paz». En un mundo así, nos estarían dejando en paz en el sentido en que se deja a un crío en el cuarto de los juguetes —con sus padres escuchando atentamente desde la habitación contigua. Ciertamente, pues, habría algo distintivamente diferente en ese mundo de control permanente, y esa diferencia ha de tenerse en cuenta en cualquier informe acerca de si esta clase de vigilancia debe ser permitida.

También deberíamos tener en cuenta el fenómeno de «las mejores intenciones». Los sistemas de vigilancia se instituyen con un motivo, pero se usan con otro. Jeff Rosen ha catalogado los abusos de la cultura de la vigilancia que ha conquistado Gran Bretaña:[15] videocámaras empleadas para mirar lascivamente a mujeres o para el sensacionalismo informativo. En EEUU, por su parte, la vigilancia masiva destinada a seguir la pista a los «terroristas» también se utilizó para seguir a grupos ecologistas o antibelicistas.[16]

Pero formulemos la cuestión en su forma más acuciante. Imaginémonos un sistema de vigilancia digital cuyo algoritmo fuera conocido y verificable, de modo que conociéramos exactamente la información que se buscó y confiáramos en que no se buscó ninguna más. Esa vigilancia sería vasta e indiscriminada, pero cualquier uso de sus resultados tendría que recibir

15 Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, Nueva York, Random House, 2004, pp. 34-53.

16 Véase American Civil Liberties Union, «The Government is Spying on Americans», disponible en http://www.aclu.org/safefree/spyfiles/index.html.

la autorización previa de un tribunal. Así pues, la máquina escupiría bits de datos implicando a X en algún crimen bajo investigación, y un tribunal decidiría si esa información basta para justificar un arresto o un registro más tradicional. Y finalmente, para hacer el sistema lo más garantista posible, la única prueba que podría extraerse de esta vigilancia sería aquélla vinculada directamente con los crímenes investigados. Así, por ejemplo, si se persigue a terroristas, las pruebas halladas no se emplearían para un proceso por evasión fiscal. No estoy especificando cuáles son los crímenes que se perseguirían; todo lo que digo es que no se usaría la regla tradicional que permite emplear toda prueba obtenida legalmente con cualquier propósito legal.

¿Violaría este sistema las protecciones de la Cuarta Enmienda? ¿Debería hacerlo?

La respuesta a esta pregunta depende de la concepción que tengamos del principio protegido por la Cuarta Enmienda. Como describí en el Capítulo 6, esta Enmienda tenía en su punto de mira los registros indiscriminados y las «órdenes generales» —es decir, los registros que no especificaban el individuo concreto al que afectaban, así como la inmunidad que se concedía a quienes los realizaban. Pero esos registros, como todos los realizados en aquella época, imponían gravámenes sobre quien los sufría. Si consideráramos que la Cuarta Enmienda protegía contra el injustificado gravamen de este registro indiscriminado, entonces esta vigilancia digital no parecería suscitar ningún problema significativo. Como expliqué más arriba, dicha vigilancia no produce gravamen alguno a menos que se descubran pruebas suficientes como para que un tribunal autorice un registro ordinario.

Ahora bien, puede que consideremos que la Cuarta Enmienda protege una especie de dignidad. Así, incluso si un registro no supone un gravamen para nadie, o incluso si resulta completamente imperceptible, esta concepción de la privacidad sostiene que la misma idea del registro supone un atentado a la dignidad. Por lo tanto, sólo si el Estado posee una buena razón para efectuar dicho registro *antes* de efectuarlo, podrá conculcar ese interés por la dignidad. Desde esta perspectiva, un registro sin justificación lesiona nuestra dignidad tanto si interfiere con nuestra vida como si no.

Yo mismo presencié el enfrentamiento abierto entre estas dos concepciones de privacidad con ocasión de un encontronazo trágicamente común en Washington DC. Un amigo y yo habíamos concertado una «ronda policial» —por la que nos dejarían acompañar a una unidad de la policía local en una de sus patrullas ordinarias. El barrio que patrullamos era uno de los más

empobrecidos de la ciudad, y alrededor de las once de la noche llegó el aviso de que una alarma de coche se había disparado cerca de donde nos encontrábamos. Cuando nos aproximamos al lugar de los hechos, vimos que al menos cinco agentes de policía estaban tratando de reducir a tres jóvenes; tres de los policías empujaron a los sospechosos contra un muro, les separaron las piernas y mantuvieron sus caras pegadas a la pared.

Los tres jóvenes eran «sospechosos» —estaban cerca de una alarma de coche cuando se disparó— pero, a la vista del cariz que tomó la cosa, cualquiera habría pensado que los habían cogido con las joyas de la Corona.

Y entonces estalló una trifulca insólita. Para sorpresa de todos, y terror mío (ya que parecía que me hallaba en medio de un polvorín, y que lo que me dispongo a describir era la chispa), uno de los tres jóvenes, de no más de diecisiete años, se dio la vuelta en un ataque de ira y comenzó a bramar contra los policías. «Cada vez que ocurre algo en este barrio, acabo tirado contra la pared con una pistola apuntándome a la cabeza. Nunca he hecho nada ilegal, pero continuamente tengo acosándome a policías con pistolas».

Uno de sus amigos se volvió e intentó calmarle. «Tranquilo, tío, sólo intentan hacer su trabajo. Será sólo un minuto y todo se habrá acabado».

«No pienso tranquilizarme. ¿Por qué cojones tengo que vivir siempre así? No soy un criminal. No merezco que me traten de esta manera. Algún día una de estas pistolas se va a disparar accidentalmente, y me convertiré en una jodida estadística. ¿Qué ocurrirá entonces?».

En ese momento intervinieron los agentes, tres de los cuales empujaron al airado joven contra el muro, manteniendo su cabeza pegada a la pared. «Será sólo un minuto. Si todo está en orden, te dejaremos libre. Relájate».

En los gritos de rabia del primer joven se expresaba el ultraje que supone la denegación de la dignidad. Sea o no razonable, suponga o no una intrusión mínima, había algo insultante en esta experiencia —más insultante aún por cuanto uno imaginaba que dicha experiencia se repetía una y otra vez. Tal y como ha escrito el juez Scalia, preguntándose si los redactores de la Constitución habrían considerado constitucional la práctica policial conocida como *Terry stop* —consistente en parar y cachear a cualquier persona cuando la policía tenga una sospecha razonable sobre ella—: «Dudo francamente [...] que los hombres profundamente orgullosos

que adoptaron nuestra Cuarta Enmienda hubieran permitido que se les sometiera, bajo la mera sospecha de ir armados y ser peligrosos, a tamaña indignidad».[17]

Y sin embargo, una vez más, nos encontramos con el argumento de la intrusión mínima. Si la privacidad es una protección contra la intromisión injustificada y excesiva, entonces en este caso no existía invasión de la privacidad. Tal y como argumentó el segundo joven, la intrusión era mínima: pasaría rápido (y así fue —a los cinco minutos habíamos abandonado el lugar, después de haberles identificado y comprobado sus antecedentes) y estaba razonablemente relacionada con un objetivo legítimo. Según esta concepción, la privacidad es simplemente la protección contra intrusiones irrazonables y onerosas, y este registro, alegó el segundo joven, no era tan irrazonable y oneroso como para justificar el ataque de ira de su amigo (que además le exponía a un peligro mucho mayor).

Desde esta perspectiva, el daño provocado por la vigilancia digital es aún más difícil de estimar. Estoy seguro de que hay personas que se sienten indignadas ante la mera idea de que se revisen registros informáticos sobre ellas, pero la mayoría de la gente reconocería que aquí está en juego una dignidad distinta. A diferencia de los desventurados muchachos puestos contra la pared, en el caso de la vigilancia digital la interferencia real es nula; pero al igual que con ellos, si no se halla nada en ese registro, no sucederá nada. Así pues, ¿en qué consiste lo indigno? ¿Cómo se expresa?

Una tercera concepción de la privacidad no atiende ni a la preservación de la dignidad ni a la minimización de la intrusión, sino que la define en términos sustantivos —la privacidad como un modo de restringir el poder regulador del Estado. En este sentido, la obra de William Stuntz proporciona una importante guía.[18] En ella Stuntz defiende que el propósito real de la Cuarta y la Quinta Enmiendas es poner demasiado difícil determinadas formas de regulación haciendo que sea materialmente imposible reunir las pruebas necesarias para aplicarlas.

Ésta es una idea que nos cuesta imaginar. En nuestro mundo, las fuentes de pruebas son abundantes —registros de tarjetas de crédito, registros telefónicos, videocámaras en el supermercado—, por lo que nos resulta difícil

---

17 Véase *Minnesota vs. Dickerson*, 508 US 366, 381, 1993 (voto coincidente del juez Antonin Scalia).

18 Véase, por ejemplo, William J. Stuntz, «Privacy's Problem and the Law of Criminal Procedure», *Michigan Law Review*, núm. 93, 1995, pp. 1016, 1026; en «The Substantive Origins of Criminal Procedure», *op. cit.*, Stuntz aborda los orígenes de la Cuarta Enmienda.

imaginar un delito del que no se pudieran reunir pruebas suficientes como para abrir una investigación criminal. Pero retrocedamos doscientos años hasta la época en que se redactó la Constitución, cuando las únicas pruebas reales eran testimonios y objetos, y el acusado tenía terminantemente prohibido testificar. Imaginémonos en este contexto que el Estado quiere castigarnos por «sedición». Nuestros escritos o nuestros propios testimonios acerca de nuestras ideas constituirían las únicas pruebas de sedición válidas a las que se podría recurrir. Por lo tanto, si esas dos fuentes quedaran eliminadas, sería prácticamente imposible tener éxito en la persecución de la sedición.

Como defiende Stuntz, esto es precisamente lo que hacen la Cuarta y la Quinta Enmienda: combinadas, imposibilitan la obtención de pruebas para un crimen como el de sedición, haciendo así inútil cualquier intento estatal de perseguirlo. Pero no sólo para la sedición —Stuntz sostiene que el efecto de la Cuarta, la Quinta y la Sexta Enmienda era la restricción del alcance de la regulación que era posible en la práctica. Como escribe este autor: «Del mismo modo que una ley que prohibiera el uso de preservativos tendería a promover el registro de dormitorios, una prohibición del registro de dormitorios tendería a desincentivar leyes que prohibieran los preservativos».[19]

Ahora bien, ¿tales registros no estaban ya restringidos, por ejemplo, por la Primera Enmienda? ¿Una ley que castigara los libelos sediciosos no habría sido inconstitucional de todas maneras? En realidad, esto no estaba nada claro en el momento de la fundación de EEUU; tan poco claro estaba que en 1798 el Congreso promulgó las Leyes de Extranjería y Sedición (*Alien and Sedition Acts*), que de hecho castigaban la sedición de forma bastante directa.[20] Muchos consideraron inconstitucionales estas leyes, pero la Cuarta y la Quinta Enmiendas habrían supuesto límites efectivos a su aplicación, fueran o no constitucionales las leyes sustantivas.

---

19 Stuntz, «Privacy's Problem and the Law of Criminal Procedure», *op. cit.*, p. 1026.

20 *Alien and Sedition Acts* de 1798, Ley de 18 de junio de 1798, cap. 59, 1, Est. 566 (derogada en 1802); Ley de 25 de junio de 1798, cap. 63, 1, Est. 570 (expirada); Ley de 6 de julio de 1798, cap. 70, 1, Est. 577 (expirada), Ley de 14 de julio de 1798, cap. 77, 1, Est. 596 (que otorgaba plenos poderes al Presidente para deportar a cualquiera que considerara peligroso para la paz y seguridad del país –expirada). Las Leyes de Extranjería y Sedición fueron declaradas inconstitucionales en *New York Times Co. vs. Sullivan,* 376 US 254, 276, 1964, aunque, por supuesto, para entonces ya habían expirado. Véase Neal Devins, *Constitutional Values*, Baltimore, Johns Hopkins University Press, 1996, sobre la revocación; y James Morton Smith, *Freedom's Fetters: The Alien and Sedition Laws and American Civil Liberties*, Ithaca (NY), Cornell University Press, 1956, sobre la historia, aplicación e impacto de las Leyes de Extranjería y Sedición.

Según esta visión, la privacidad se concibe como un límite sustantivo al poder estatal.[21] Así entendida, la privacidad va más allá de proteger la dignidad o limitar la intrusión; la privacidad restringe lo que el Estado puede hacer.

Si ésta fuera nuestra concepción de la privacidad, entonces la vigilancia digital la podría tener en cuenta. Si hubiera ciertos crímenes cuya persecución fuera inadecuada, podríamos eliminarlos del algoritmo de búsqueda. Sería complicado identificar qué crímenes han de ser eliminados del algoritmo en virtud de la Constitución —la Primera Enmienda ya veta claramente la sedición de la lista. Quizá la norma simplemente sigue la pista de la limitación constitucional.

Ahora la clave está en reconocer que, en principio, estas tres concepciones distintas de la privacidad podrían arrojar resultados diferentes dependiendo del caso. Por ejemplo, puede que un registro no incurra en una intrusión pero ofenda la dignidad. En ese caso, tendríamos que escoger aquella concepción de la privacidad que creyésemos que expresa mejor la protección consagrada en la Constitución.

En la época en que se redactó, sin embargo, estas distintas concepciones de la privacidad no habrían producido, en general, conclusiones diferentes. Cualquier registro que sobrepasase los límites sustantivos de la Enmienda, o los de la dignidad, habría supuesto también un trastorno para el ciudadano. La mitad de los redactores de la Constitución podría haber defendido la concepción basada en la dignidad y la otra mitad podría haber defendido la basada en la utilidad, pero como todo registro habría supuesto una violación de ambas, todos los redactores podrían haber aprobado las protecciones de la Cuarta Enmienda.

Hoy, sin embargo, esto ya no es así. Hoy las tres concepciones podrían arrojar resultados muy dispares. La concepción utilitarista podría permitir registros eficaces prohibidos por las otras dos concepciones. La traducción correcta (en el sentido en que Brandeis empleó el término en el caso de los pinchazos telefónicos) depende de la elección de una concepción adecuada con la que traducir.

En este sentido, nuestras protecciones originales fueron el producto de lo que Cass Sunstein llama un «acuerdo incompletamente teorizado».[22] Dada la tecnología de la época, no había razón para desarrollar teóricamente los

---

21 Stuntz, «Substantive Origins», *op. cit.*, p. 395.

22 Véase Cass Sunstein, *Legal Reasoning and Political Conflict*, Oxford, Oxford University Press, 1996, pp. 35-61.

fundamentos del texto constitucional; las tres teorías eran coherentes con la tecnología existente. Pero a medida que la tecnología cambia, dicho contexto original se ve cuestionado. Ahora que tecnologías como el *gusano* pueden registrarnos sin llegar a importunarnos, emerge un conflicto acerca de qué es lo que protege la Cuarta Enmienda.

Este conflicto constituye el reverso del acuerdo incompletamente teorizado de Sunstein. Podríamos afirmar que en cualquier acuerdo incompletamente teorizado existirán ambigüedades latentes, y podemos describir contextos donde dichas latencias emerjan. Las ambigüedades latentes en torno a la protección de la privacidad, por ejemplo, quedan patentes por la evolución de la tecnología. Y eso, a su vez, nos obliga a elegir.

Una vez más, algunos apuntarán que esa decisión ya ha sido tomada —por nuestra Constitución, en nuestro pasado. Ésta es la retórica de buena parte de nuestra jurisprudencia constitucional, pero dicha retórica no resulta aquí de gran ayuda. No creo que los redactores de la Constitución establecieran lo que la Enmienda protegería en un mundo donde pudieran llevarse a cabo registros que no supusieran invasión alguna. No concibieron una constitución aplicable a todos los mundos posibles, sino una que fuera de aplicación en el suyo. Cuando su mundo difiere del nuestro de una forma que supone una elección a la que ellos no se enfrentaron, entonces, nos corresponde decidir a nosotros.

Privacidad en público: datos

La historia que he explicado hasta el momento trata sobre los límites respecto al Estado: ¿Qué poder debería tener el Estado para vigilar nuestras actividades, al menos cuando éstas se realizan en público? He aquí el interrogante especial que suscita el ciberespacio: ¿Qué límites deberían imponerse a la «vigilancia digital»? Existen, por supuesto, otras muchas preguntas tradicionales que también son importantes, pero mi interés se centra en la «vigilancia digital».

En esta parte voy a considerar un tercer interrogante sobre la privacidad que, pese a estar íntimamente relacionado con lo anterior, es muy distinto. Se trata del interrogante acerca de qué presuntos controles deberíamos tener sobre los datos que revelamos a los demás. Aquí ya no se trata fundamentalmente del control estatal, por lo que la pregunta va más allá del

alcance habitual de la Cuarta Enmienda. En lugar del Estado, dichos controles se ejercen sobre actores privados que, o bien han reunido información sobre mí mientras me observaban, o bien han recopilado dicha información de mí mismo.

Una vez más, comencemos analizando esto desde la perspectiva del espacio real. Si yo contrato a un detective privado para seguir al lector, no violo ningún derecho de nadie. Si elaboro una lista con los lugares adonde ha ido el lector, no hay nada que me impida venderla. Puede que el lector piense que esto supone una intrusión, y que es indignante que la ley permita que ocurra algo así. Pero insisto en que tradicionalmente la ley no ha prestado mucha atención a este tipo de invasión, ya que los costes de tal vigilancia eran demasiado elevados. Acaso las celebridades y los famosos desearían que las reglas fueran diferentes, pero para la mayoría de nosotros, durante la mayor parte de nuestra historia, no había necesidad de que la ley interviniese.

El mismo razonamiento podría aplicarse a los datos que yo cedía a empresas u otras entidades en la época previa a Internet. No había nada en la ley que limitase lo que dichas entidades hacían con mis datos: podían venderlos a empresas o a corredores de listas de envíos postales, o usarlos del modo que quisieran. De nuevo, el coste práctico de emplear la información era elevado, por lo que el empleo que se le daba era escaso. Y lo más importante, la invasión que suponía cualquiera de esos usos de mis datos era relativamente reducida. El producto principal que se extraía de ellos era el correo basura, y éste no suponía un gravamen significativo en el espacio físico.

Pero ahora, con la «vigilancia digital», las cosas han cambiado drásticamente. Las dos historias siguientes nos permitirán hacernos una idea de este cambio:

– A comienzos de 2006, el *Chicago Sun-Times* informó[23] de que existían sitios web que vendían los registros telefónicos de llamadas realizadas desde teléfonos móviles. Un *blog* llamado AmericaBlog constató los hechos adquiriendo el registro telefónico del mismísimo General Wesley Clark. Por unos 120 dólares, el *blog* logró demostrar lo que la mayoría de

23 Frank Main, «Blogger Buys Presidential Candidate's Call List», *Chicago Sun-Times*, 13 de enero de 2006, disponible en http://www.suntimes.com/output/news/cst-nws-cell13.html.

la gente consideraba imposible: que cualquiera provisto de una tarjeta de crédito podría encontrar algo tan personal como la lista de personas a las que alguien llama desde un móvil (así como la frecuencia y la duración de dichas llamadas).

Esta conducta era tan escandalosa que nadie realmente salió en su defensa, pero no habría sido complicado hacerlo. Wesley Clark marcó «voluntariamente» los números en su teléfono móvil, con lo que cedió voluntariamente esa información a la compañía telefónica. Y gracias a que ésta podía vender dichos datos, sus tarifas podían mantenerse (más) bajas. Clark se beneficiaba de estas tarifas bajas, así pues, ¿de qué se quejaba?

– Hace años recibí una carta de AT&T. Iba dirigida a una antigua novia, pero no la habían reenviado a su nueva dirección sino al piso donde yo vivía por entonces. AT&T quería ofrecerle una nueva tarjeta de crédito, pero llegaba un poco tarde: ella y yo habíamos roto hacía ocho años. Desde entonces, ella se había mudado a Texas y yo a Chicago, a Washington, de nuevo a Chicago, luego a New Haven, de nuevo a Chicago, y finalmente a Boston, donde había cambiado dos veces de domicilio. Pero lo errante de mi vida no disuadió a AT&T, que, con gran fe en mi constancia, creyó que una mujer a la que no veía desde hacía ocho años compartía piso conmigo.

¿Cómo es que AT&T mantuvo tal creencia? Bueno, en el ciberespacio hay flotando montones de datos sobre mí recopilados desde el mismo momento en que empecé a usar tarjetas de crédito, teléfonos y quién sabe qué otra cosa. El sistema trata continuamente de actualizar y refinar esta extraordinaria colección de datos —es decir, traza mi perfil y, a partir de él, determina el modo de interactuar conmigo.

Estas historias no son más que la punta del iceberg. Todo lo que hacemos en Internet genera datos, los cuales, en conjunto, son extremadamente valiosos, más aún para el comercio que para el Estado. A este último (en circunstancias normales) sólo le preocupa realmente que obedezcamos un selecto conjunto de leyes, pero el comercio tiene mucho interés en conocer cómo queremos gastar nuestro dinero, y esos datos se lo permiten. A partir de las masivas cantidades de datos disponibles sobre lo que hacemos y decimos, cada vez es más factible vendernos mercancías de un modo directo y efectivo. Gmail realiza un tratamiento de los datos de nuestra cuenta de correo electrónico para ver qué debería tratar de vendernos. Amazon examina los productos

que hojeamos en su página para ver qué ofertas especiales *Gold Box* puede lanzar. Hay una lista interminable de entidades que desean saber más de nosotros para servir mejor (como mínimo) a sus intereses. ¿Qué límites, o restricciones, deberían imponérseles?

Deberíamos comenzar con un argumento obvio que podría contribuir a orientar nuestra respuesta. Hay una gran diferencia entre (1) recopilar información sobre X para dilucidar un crimen o descubrir a un criminal, (2) recopilar información sobre X que se le venderá a Y simplemente para revelarle ciertos hechos sobre X (como sus llamadas de móvil) y (3) recopilar información sobre X para venderle mejor a X. En los casos (1) y (2), X sale perjudicado, aunque si creemos que el crimen es realmente un crimen, en el caso (1) X no estaría peor de lo que debería estar. En principio, el caso (3) podría beneficiar a X —ya que facilita una publicidad mejor dirigida y diseñada para promocionar transacciones voluntarias. Digo «en principio» porque aunque es posible que los anuncios estén mejor dirigidos a X, también recibirá más cantidad de ellos. En resumidas cuentas, puede que X salga más perjudicado con la avalancha de ofertas más personalizadas que con una menor cantidad de ellas más genéricas. Pero a pesar de esa posibilidad, la motivación del caso (3) es diferente a las de los casos (1) y (2), y ello podría influir en buena medida en el modo en que deberíamos responder a la pregunta anterior.

Comencemos, pues, centrándonos en el caso (3): ¿Qué perjuicio provoca esta forma de «invasión»? Enconados argumentos surgen de un lado y del opuesto.

El bando que defiende que «no hay ningún perjuicio» asume que el equilibrio de la privacidad se respeta porque es la persona la que revela públicamente información sobre sí misma. Por supuesto que la ley debería proteger aquella información custodiada bajo llave o escrita en un diario privado; pero cuando alguien la expone públicamente, cuando realiza transacciones o envía material en público, renuncia a cualquier derecho a la privacidad. Por lo tanto, desde ese momento, otras personas tienen derecho a recopilar información sobre la conducta pública de ese alguien y a hacer con ella lo que más les convenga.

¿Por qué tal idea no preocupa a estos teóricos? Las razones son numerosas:

– La primera razón es que el perjuicio no es muy grande. El lector se saca la tarjeta de descuento del supermercado de su barrio, y éste recopila con ella información sobre lo que compra. Con esa información, el supermercado

puede venderle diferentes productos o calcular cómo establecer mejor sus precios; incluso puede decidir que debería ofrecer distintas combinaciones de descuentos para dar un mejor servicio a sus clientes. Estas respuestas, continúa el argumento, son las únicas probables, puesto que el supermercado no tiene más propósito que vender sus productos de forma más eficaz.

– La segunda razón es que obligar a los demás a ignorar lo que alguien les muestra supone una carga injusta para ellos. Que los demás no puedan usar la información sobre nosotros equivale a exigirles que desechen algo que hubiéramos depositado en su terreno. Así pues, si no queremos que los demás usen dicha información, no la pongamos en sus manos.

– La tercera razón es que en realidad esta información sirve para algo bueno. No sé por qué Nike cree que soy la persona adecuada para opinar sobre sus últimas zapatillas, ni tampoco por qué la marca de deportivas que uso no acierta nunca a consultarme. En ambos casos, sospecho que el motivo es que los datos que tienen sobre mí son erróneos. Me encantaría que Nike supiera lo suficiente sobre mí como para dejarme en paz; y así lo haría si esos datos se recopilasen y clasificasen mejor.

– Finalmente, en general las empresas no gastan dinero en recopilar esta información para conocernos realmente mejor, sino para conocer mejor a gente *como nosotros*. Quieren adscribirnos a una tipología de cliente. En principio, a las empresas les encantaría conocer qué tipo de persona somos, incluso si no pudieran llegar a saber más de nosotros. Lo que buscan los comerciantes es un modo de discriminar —exclusivamente en el sentido de ser capaces de diferenciar entre distintos tipos de personas.

No obstante, el otro bando de esta discusión también tiene su parte de razón. Éste comienza, una vez más, señalando los principios protegidos originalmente por la imperfección de la tecnología de control. Esta imperfección contribuía a preservar principios sustantivos importantes, como la propia presunción de inocencia. En un momento dado, hay hechos inocentes sobre nosotros que pueden aparecer, en un contexto o escenario específico, como inculpatorios. Peter Lewis, en artículo publicado en el *New York Times* bajo el título «Forget Big Brother» [Olvida al Gran Hermano], expresa bien esta idea:

> Las cámaras de vigilancia siguieron a la atractiva joven rubia por el vestíbulo del céntrico hotel de Manhattan, mantuvieron una mirada vidriosa sobre ella cuando tomó el ascensor para subir al piso 23 y otearon discretamente el pasillo en el momento en que llamó a la puerta de mi habitación. No he visto las

> cintas, pero puedo imaginarme el código de tiempos digital desplegado sobre las imágenes, indicando la hora exacta del encuentro. Todo esto vendría muy bien si alguien pretendiera cuestionar más tarde por qué esta mujer, que no es mi esposa, acudió a visitarme a mi habitación de hotel durante un reciente viaje de negocios. Luego las cámaras nos vieron dirigiéndonos a cenar y luego al teatro —un tejano casado de mediana edad abrazado a una linda mujer del East Village neoyorquino que bien podría ser su hija.

«De hecho», escribe Lewis, «era mi hija».[24]

Una lección de esta historia es el gravamen que imponen estos hechos controlados. La carga de la prueba recae sobre nosotros, los controlados, para, en primer lugar, demostrar nuestra inocencia y, en segundo lugar, asegurar que somos inocentes a todos los que pudieran considerar ambiguos estos mismos hechos. Ambos procesos, sin embargo, resultan imperfectos, ya que por más que digamos, las dudas permanecerán ahí. Siempre habrá gente que no se crea nuestro alegato de inocencia.

El control moderno no hace más que exacerbar este problema. Así, nuestra vida se convierte en un registro perpetuo, donde nuestras acciones quedan almacenadas para siempre, disponibles para ser reveladas en cualquier momento y, por consiguiente, susceptibles de ser puestas en tela de juicio.

Un segundo principio se deriva directamente de esta moderna capacidad para archivar datos. Todos nosotros deseamos vivir en comunidades separadas, o entre o dentro de espacios normativos separados. La privacidad, o la capacidad de controlar la información sobre uno mismo, respalda dicho deseo, permitiendo la coexistencia de estas múltiples comunidades e inhabilitando el poder de una comunidad dominante para imponer sus normas sobre las demás. Pensemos, por ejemplo, en un hombre gay en una pequeña ciudad intolerante.

Este principio se comprende más claramente cuando se lo contrasta con un argumento avanzado por David Brin.[25] Brin refuta esta preocupación por la privacidad —al menos si la privacidad se define como la necesidad de bloquear la producción y distribución de información sobre otras personas; y lo hace porque está convencido de que tal objetivo es imposible: el genio ya está fuera de la botella. Mejor será, sugiere Brin, encontrar formas de asegurar

---

24 Peter H. Lewis, «Forget Big Brother», *New York Times*, 19 de marzo de 1998, G1.

25 Brin, *The Transparent Society*, *op. cit.*, pp. 8-15.

que tal capacidad de recopilación de datos esté al alcance de todos. De este modo, la solución al hecho de que alguien me espíe ya no será el bloqueo, sino el permiso para el *contraespionaje* —para así pedirle cuentas a ese alguien, quizá por su espionaje o quizá por cualquier otra cosa que pueda estar haciendo.

Existen dos respuestas para este argumento. Una plantea la pregunta: ¿por qué tenemos que escoger? ¿Por qué no podemos controlar el espionaje e incorporar inspecciones en la distribución de técnicas de espionaje?

La otra respuesta atañe a lo fundamental. Brin asume que este contraespionaje sería útil para la «exigencia de responsabilidades», pero ¿según qué normas? La «exigencia de responsabilidades» es un término benigno sólo en la medida en que confiemos en la comunidad que la lleva a cabo. Cuando vivimos en múltiples comunidades, dicha exigencia se convierte en un instrumento para que una comunidad imponga a otra su visión de lo correcto. Puesto que no vivimos en una única comunidad, no vivimos según un único sistema de valores, y la exigencia de responsabilidad perfecta sólo puede socavar tal combinación de valores.

La imperfección del control actual posibilita esta multiplicación de comunidades normativas. La capacidad de arreglárselas sin un registro perfecto posibilita una diversidad que el conocimiento perfecto suprimiría.

Un tercer principio surge también de la preocupación por la elaboración de perfiles. Si buscamos en Google «hipoteca», en nuestra pantalla aparecen anuncios de hipotecas; y lo mismo sucede si buscamos sexo o coches. La publicidad está vinculada a la búsqueda que realizamos. En este sentido, se recopilan datos, pero éstos van más allá de la información sobre nuestra búsqueda. Así, hay diferentes sitios que recopilan minuciosamente toda la información personal posible sobre nosotros.[26] Y cuando enlazamos la búsqueda de Google a una página web, esa búsqueda que acabamos de efectuar se transfiere al siguiente sitio.

26 Para una buena historia que resume efectivamente el estado de la publicidad web, y para una discusión sobre el funcionamiento de DoubleClick y un caso de estudio de la venta de proyectores de 3M a través de la empresa de emplazamiento de publicidad, véase Aquantive, disponible en http://www.aquantive.com y 24-7 Real Media, disponible en http://www.247realmedia.com.

La recopilación de datos es la actividad dominante de los sitios web comerciales. En torno al 92 % recopila datos de los usuarios de su web que luego aglutina, clasifica y usa.[27] Oscar Gandy denomina esto la «clasificación panóptica» —una vasta estructura de recopilación de datos y de discriminación a partir de ellos—, y es dicha discriminación, afirma él, la que debería preocuparnos.[28]

Pero, ¿por qué? Dejemos de lado una importante clase de problemas —el uso indebido de los datos— y limitémonos a considerar su uso ordinario. Como afirmé antes, el principal efecto de dicha clasificación es simplemente hacer que el mercado funcione de forma más fluida: los intereses y productos se acomodan a la gente de un modo más certero y menos intrusivo del que existe hoy. Imaginémonos un mundo donde los publicistas pudieran establecer qué espacios publicitarios son rentables y cuáles no, donde resultara ineficaz anunciarse en vallas publicitarias o en programas masivos y la mayoría de la publicidad fuera certera y específica. En ese mundo sería más probable que la publicidad llegara a aquéllos para los que resultara útil. O eso es al menos lo que se argumenta. Sin duda, esto es discriminación, pero no del tipo de la de Jim Crow,[29] sino la maravillosa clase de discriminación que me ahorra los anuncios de Nike.

Pero más allá de una preocupación quizá efímera acerca de cómo afectan esos datos a los individuos, la elaboración de perfiles suscita una preocupación colectiva más amplia acerca de cómo podrían llegar a afectar a una comunidad.

Esta preocupación se refiere a la manipulación. Puede que seamos escépticos ante el poder de la publicidad televisiva para controlar los deseos de la gente: la televisión es muy obvia y sus motivos están muy claros. Pero ¿qué sucede cuando los motivos no son tan obvios, cuando parece como si las

---

27 Véase Federal Trade Commission, «Privacy Online: A Report to Congress», junio 1998, núm. 107, disponible en http://www.ftc.gov/reports/privacy3/toc.htm.

28 Véase Gandy, *The Panoptic Sort*, *op. cit.*, pp. 1-3.

29 Con el nombre de Jim Crow se designa, en EEUU, la política de segregación y discriminación de la población negra que fue impulsada especialmente a través de las leyes aprobadas en los Estados del Sur a finales del siglo XIX y que no fue puesta en cuestión hasta después de la Segunda Guerra Mundial. El término proviene del título de una canción de las plantaciones compuesta por el trovador Thomas «Daddy» Rice en torno a 1830. En ella, Rice ridiculizaba a los esclavos negros a través del personaje de Jim Crow, que adquirió una gran popularidad como símbolo de la pretendida inferioridad racial de los negros [N. del E.].

opciones aparecieran justo cuando las quieres? Cuando el sistema parece saber lo que queremos mejor, e incluso antes, que nosotros mismos, ¿cómo saber de dónde provienen realmente esos deseos?

Si esta posibilidad es realista, o si debería constituir una preocupación, son cuestiones complicadas que permanecen abiertas. Steven Johnson sostiene de forma bastante convincente que estos agentes de elección facilitarán un abanico y una diversidad de opciones mucho mayor —incluso, en parte, derivando en caos.[30] Ahora bien, existe también otra posibilidad —que los perfiles comiencen a normalizar a la población de la que se extrae la norma. El observador influirá así en el observado. El sistema examina lo que hacemos y nos encasilla en un patrón; ese patrón se nos reintroduce a continuación en forma de opciones establecidas por él mismo; esas opciones refuerzan el patrón, y el ciclo comienza de nuevo.

Una segunda preocupación concierne a la igualdad. La elaboración de perfiles suscita un interrogante que permanecía latente en el mercado hasta hace muy poco. Durante buena parte del siglo XIX, el pensamiento económico estadounidense estaba animado por un ideal de igualdad. En el espacio civil, todos los individuos eran considerados iguales, todos podían comprar, vender y aproximarse a otros en pie de igualdad. Puede que se conocieran hechos acerca de los individuos, y que alguno de ellos pudiera inhabilitarles para algunas transacciones económicas —una bancarrota anterior, por ejemplo, podría inhabilitar a alguien para hacer transacciones en el futuro—, pero, en general, existían espacios de relativo anonimato donde podían efectuarse transacciones económicas.[31]

Con el paso del tiempo, este espacio de igualdad ha quedado desplazado por la creación de *zonas* económicas que persiguen la segregación,[32] es decir, por leyes que promueven las distinciones basadas en criterios sociales

---

30 Johnson, *Interface Culture*, *op. cit.*, pp. 192-205. Andrew Shapiro denomina esto el «efecto de retroalimentación», pero defiende que limita el abanico de opciones; véase Andrew Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, Nueva York, PublicAffairs, 1999, p. 113 [ed. cast.: *El mundo en un clic: cómo Internet pone el control en sus manos (y está cambiando el mundo que conocemos)* trad. por Francisco J. Ramos Mena, Barcelona, Grijalbo Mondadori, 2001].

31 Véase, por ejemplo, *McIntyre vs. Ohio Elections Commission*, 514 US 334, 341-343, 1995.

32 Véase Janai S. Nelson, «Residential Zoning Regulations and the Perpetuation of Apartheid», *UCLA Law Review*, núm. 43, 1996, pp. 1689, 1693–1704.

o económicos.[33] El ejemplo más patente de ello es la propia zonificación geográfica. No fue hasta el siglo XX que las leyes locales se utilizaron para ubicar a la gente en espacios segregados.[34] Al principio, esta legislación tenía una base racial, pero cuando se abolió la zonificación basada en la raza, las técnicas de zonificación se transformaron.[35]

Es interesante recordar lo controvertido que resultó este uso de la ley.[36] Para muchos, tanto ricos como pobres, constituía una afrenta al ideal estadounidense de igualdad que tu lugar de residencia dependiera de cuánto dinero tenías. Qué duda cabe que eso es siempre así cuando la propiedad es algo que debes comprar, pero las leyes de zonificación añadían el respaldo de la ley a la segregación impuesta por el mercado. El efecto de esto es la recreación en la ley, y por ende en la sociedad, de distinciones entre las personas.

Hubo una época en que habríamos definido EEUU como un lugar que pretendía borrar tales distinciones. El historiador Gordon Wood describe este propósito como un elemento importante de la revolución que llevó al nacimiento del país.[37] El enemigo entonces era la jerarquía social y legal, y el fin era alcanzar una sociedad igualitaria. La revolución constituyó un ataque a las jerarquías de rango social y a los privilegios derivados de ellas.

---

33 Ejemplos de leyes que persiguen la segregación basada en criterios sociales o económicos son: regulaciones que exigen una mínima superficie de terreno para las viviendas; ordenanzas que prohíben que familias «no tradicionales» vivan en ciertas áreas; y clasificaciones residenciales que excluyen la construcción de pisos. Todas estas restricciones incrementan significativamente el coste de la vivienda para individuos de rentas más bajas; véase *ibidem*, pp. 1699–1700.

34 En 1926 el Tribunal Supremo respaldó la zonificación como un ejercicio válido de poder por parte de las autoridades locales. Véase *Village of Euclid vs. Ambler Realty Company,* 272 US 365, 1926, donde se sostiene que un Estado tiene derecho a separar usos incompatibles. No fue hasta el siglo XX que se otorgó a los municipios poder suficiente para regular áreas legales como las concernientes a decisiones de zonificación; véase Richard Briffault, «Our Localism: Part I—The Structure of Local Government Law», *Columbia Law Review*, núm. 90, 1990, pp. 1, 8-11, 19.

35 En 1917 el Tribunal Supremo proscribió la zonificación racial por incurrir en una violación de la Decimocuarta Enmienda; véase *Buchanan vs. Warley,* 245 US 60, 1917. Sin embargo, la regulación zonificadora «no excluyente» se siguió usando para preservar la segregación residencial; aunque racialmente neutrales y basadas en factores económicos (ostensiblemente para impedir la devaluación de las propiedades), diversas leyes y regulaciones han resultado *de facto* segregadoras; véase Briffault, «Our Localism», *op. cit.*, pp. 103-104; Meredith Lee Bryant, «Combating School Resegregation Through Housing: A Need for a Reconceptualization of American Democracy and the Rights It Protects», *Harvard BlackLetter Journal*, núm. 13, 1997, pp. 127, 131-132.

36 Véase Joel Kosman, «Toward an Inclusionary Jurisprudence: A Reconceptualization of Zoning», *Catholic University Law Review*, núm. 43, 1993, pp. 59, 77-86, 101-103.

37 Véase Gordon S. Wood, *The Radicalism of the American Revolution*, Nueva York, Alfred A. Knopf, 1992, pp. 5-8, 271-286.

Toda jerarquía social necesita suficiente información previa para poder efectuar discriminaciones de rango, lo que exigía, históricamente, grupos sociales bastante estables. Así, para realizar sutiles distinciones de clase —por ejemplo, para saber si un joven bien vestido era el caballero que afirmaba ser o un simple comerciante disfrazado— se requería conocer los acentos, modas, costumbres y maneras locales, por lo que sólo donde existiera una movilidad social relativamente escasa podrían imponerse estos sistemas jerárquicos.

En consecuencia, a medida que se incrementaba la movilidad, dichos sistemas jerárquicos comenzaron a ser desafiados. Más allá de los extremos de la gente muy rica o muy pobre, la capacidad para efectuar sutiles distinciones de rango desapareció a medida que la movilidad y la fluidez de la sociedad las dificultaban cada vez más.

La elaboración de perfiles viene a cambiar todo esto. Un sistema eficaz y efectivo de control posibilita de nuevo la realización de dichas sutiles distinciones de rango; la recopilación de datos barata y eficaz nos llevará, pues, de vuelta al pasado. Pensemos en los programas de fidelización de las compañías aéreas para sus viajeros frecuentes. Todo el mundo comprende la característica obvia de dichos programas —los vuelos gratuitos para viajeros frecuentes. En sí mismos, tales programas de reembolso resultan bastante inocuos, siendo su parte más interesante el poder que otorgan a las compañías aéreas para discriminar en sus servicios.

Cuando una viajera frecuente reserva un vuelo, la reserva incluye un perfil de cliente. Este perfil puede abarcar información acerca del asiento que prefiere o si le gusta la comida vegetariana, y también indica con qué frecuencia vuela esa persona. Algunas compañías aéreas pueden luego efectuar discriminaciones sobre la base de esta información. La forma más obvia de hacerlo es mediante la situación de los asientos —los viajeros frecuentes consiguen mejores asientos—, pero puede que esa información influya también en la distribución de la comida durante el vuelo —los viajeros frecuentes más habituales eligen primero, y puede que los demás tengan que conformarse con lo que reciban.

Dentro del proyecto de justicia social, por supuesto, estos privilegios no son más que menudencias, pero mi argumento es más general. Los sistemas de fidelización de viajeros permiten la recreación de sistemas de estatus, ya que proporcionan información sobre los individuos que las organizaciones

podrían valorar, y usar, a la hora de dispensar sus servicios.[38] Posibilitan la discriminación porque restauran la información que la movilidad había destruido, constituyendo así un modo de frustrar una de las ventajas del anonimato —la ventaja de la igualdad.

Los economistas responderán que en muchos contextos esta capacidad de discriminar —de ofrecer bienes a diferentes precios a distinta gente— supone en conjunto un beneficio,[39] por lo que, en términos generales, la gente está mejor si se le ofrece la discriminación de precios que si no se le ofrece. Así pues, podrían concluir estos economistas, estaremos mejor si facilitamos en la medida de lo posible dicha discriminación.

Pero estos principios no son más que uno de los términos de la ecuación, hay que contrapesarlos con los principios de igualdad. Puede que estos principios nos parezcan antiguos, pero no deberíamos suponer que, sólo porque sean lejanos hoy, lo ha sido siempre.

Tomemos como ejemplo las propinas. Por más benigna (aunque molesta) que podamos considerar la práctica de dar propinas, hubo una época en el tránsito del siglo XIX al XX en que su sola idea suponía un insulto, una ofensa a la dignidad de un ciudadano libre. Viviana Zelizer lo describe así:

> A comienzos del siglo XX, a medida que las propinas se hacían cada vez más populares, provocaron una gran controversia moral y social. De hecho, por toda la nación las asambleas legislativas estatales se esforzaron, a veces con éxito, por abolirlas, convirtiendo el dar propina en una falta punible. En incontables editoriales de periódicos y artículos de revistas, en los libros de etiqueta, e incluso en los tribunales, las propinas estaban sometidas a un severo examen con una mezcla de curiosidad, diversión y ambivalencia —y a menudo de hostilidad abierta. Cuando, en 1907, el Gobierno sancionó oficialmente las propinas

---

38 Véase Lynne G. Zucker, «Production of Trust: Institutional Sources of Economic Structure, 1840-1920», *Research in Organizational Behavior*, núm. 8, 1986, p. 53.

39 La discriminación de precios es la capacidad para cobrar el mismo bien a diferentes precios. Los billetes de avión son el mejor ejemplo de ello: el mismo asiento puede costar cientos de dólares más a un viajero que no puede quedarse a dormir la noche del sábado. Véase, por ejemplo, Joseph Gregory Sidak, «Debunking Predatory Innovation», *Columbia Law Review*, núm. 83, 1983, pp. 1121, 1132-1135; véase también Easterbrook, «Intellectual Property Is Still Property», *op. cit.*; Fisher, «Reconstructing the Fair Use Doctrine», *Harvard Law Review*, núm. 101, 1998, p. 1659; pero véase Janusz A. Ordover *et al.*, «Predatory Systems Rivalry: A Reply», *Columbia Law Review*, núm. 83, 1983, pp. 1150, 1158-1164.

> al permitir que oficiales y reclutas de la Marina estadounidense las incluyeran como un apartado más de sus dietas de viaje, esta decisión fue denunciada como un espaldarazo ilegítimo a la corrupción. Periódicamente se producían llamamientos a organizar ligas antipropinas.[40]

Existe una concepción de la igualdad que quedaría corrompida por la eficacia que ha alcanzado la elaboración de perfiles. Tal concepción constituye un principio que ha de contrapesarse con la mencionada eficacia. Aunque yo esté convencido de que este principio es relativamente débil en la vida estadounidense, ¿quién soy yo para decirlo? Lo importante aquí no es la fortaleza o debilidad del principio, sino la tensión o el conflicto que permanece latente hasta que lo revela la emergencia de la tecnología de elaboración de perfiles.

A estas alturas, el patrón debería resultarnos familiar, ya que hemos contemplado este cambio en otros ámbitos. Una vez más, el código cambia y, al hacerlo, pone de relieve un conflicto de principios. Mientras que antes existía una igualdad relativa porque la información que permitía discriminar era demasiado cara de obtener, ahora la discriminación sale rentable. La diferencia —lo que hace que salga rentable— es la emergencia de un nuevo código: el código cambia, cambia la conducta, y un principio latente en el régimen anterior queda desplazado.

Podríamos reaccionar trabando el código para preservar ese régimen anterior. También podríamos crear restricciones constitucionales o legales que impidan el paso al nuevo mundo. O bien podríamos hallar formas de reconciliar este mundo emergente con los principios que consideramos fundamentales.

Soluciones

A lo largo de este capítulo, he identificado dos amenazas distintas que Internet crea a los principios de privacidad. La primera es la amenaza de la «vigilancia digital» —la creciente capacidad del Estado (entre otros) de

40 Viviana A. Zelizer, *The Social Meaning of Money* (2ª), Princeton, Princeton University Press, 1994, pp. 94-95.

«espiar» nuestras actividades «en público». Desde el acceso a Internet hasta un simple paseo por la calle, pasando por el correo electrónico y las llamadas de teléfono, la tecnología digital está brindando la oportunidad de llevar a cabo registros exentos de molestias y cada vez más perfectos.

La segunda amenaza proviene del creciente acopio de datos por parte de entidades privadas (entre otras), no tanto para «espiar» sino para facilitar el comercio. Una parte de este comercio explota la fuente de los datos (los números a los que Wesley Clark llamó desde su móvil); otra parte trata de facilitar el comercio con dicha fuente (mediante anuncios segmentados).

Ante estos dos riesgos diferentes, podemos imaginar cuatro tipos de respuesta, cada uno de los cuales mapea una de las modalidades que describí en el Capítulo 7:

– Ley. La regulación legal podría diseñarse para responder a estas amenazas. Analizaremos algunas de esas regulaciones más adelante, pero la forma general debería estar bastante clara. La ley podría, por ejemplo, ordenar al Presidente de EEUU que no vigilase a los ciudadanos sin contar con sospechas razonables (que el Presidente cumpla la ley es una cuestión aparte); o podría prohibir la venta de datos recopilados de clientes sin su consentimiento expreso. En ambos casos, la ley amenaza con sanciones para modificar la conducta de forma directa. El objetivo de la ley podría ser tanto aumentar el poder de los individuos para controlar sus datos personales como para anularlo (por ejemplo, ilegalizando ciertas transacciones relacionadas con la privacidad).

– Normas. Las normas también podrían usarse para responder a estas amenazas. Así, por ejemplo, las normas entre entidades comerciales podrían contribuir a construir confianza en torno a ciertas prácticas protectoras de la privacidad.

– Mercados. De formas que se verán más claras a continuación, el mercado podría usarse para proteger la privacidad de los individuos.

– Arquitectura/Código. La tecnología podría usarse igualmente para proteger la privacidad. A menudo nos referimos a estas herramientas como «tecnologías de aumento de la privacidad» (PET, acrónimo de *Privacy Enhancing Technologies*), tecnologías diseñadas para proporcionar al usuario un mayor control técnico sobre los datos asociados a él o ella.

Como vengo defendiendo reiteradamente, no existe una solución única para los problemas políticos en Internet. Toda solución requiere una combinación de al menos dos modalidades, y mi objetivo en lo que queda de capítulo es describir una combinación para cada una de estas amenazas a la privacidad.

Qué duda cabe que esta combinación resultará controvertida para algunos. No obstante, mi propósito no es tanto propugnar una combinación particular dentro de este conjunto de modalidades como contrastar un determinado enfoque. No insisto, pues, en las soluciones concretas que propongo, sino en que las soluciones en el contexto del ciberespacio son el producto de tal combinación.

Vigilancia

El Estado vigila todo lo que puede en su lucha contra lo que sea que esté luchando ahora. Cuando esa vigilancia es obra de humanos —las escuchas telefónicas, o algo por el estilo—, entonces deberían aplicarse los límites legales tradicionales. Esos límites imponen costes (y, por lo tanto, usando el mercado, reducen la incidencia a los casos más significativos), garantizan al menos algún tipo de revisión y, acaso lo más importante, construyen en el seno de la aplicación de la ley una norma de respeto al procedimiento.

Ahora bien, cuando esa vigilancia es digital, entonces estimo que debería aplicarse un conjunto de restricciones diferente. Así, la ley debería sancionar la «vigilancia digital» si, *y sólo si*, se dan una serie de condiciones:

1. Que se describa el propósito del registro habilitado en el algoritmo de búsqueda.

2. Que se revise la función del algoritmo.

3. Que se certifique que el propósito del registro coincide con la función del algoritmo.

4. Que no pueda llevarse a cabo ninguna acción —incluyendo un registro subsiguiente— contra un individuo basándose en el algoritmo sin que exista supervisión judicial.

5. Que, salvo en contadas excepciones, no pueda emprenderse ninguna acción contra un individuo por motivos ajenos al propósito descrito. Por consiguiente, si se buscan pruebas de tráfico de drogas, no pueden usarse las pruebas halladas para perseguir el fraude con tarjetas de crédito.

He aquí las restricciones legales aplicables al Estado con el fin de aumentar la privacidad. Si éstas fueran satisfechas, entonces, a mi modo de ver, tal vigilancia digital no tendría por qué entrar en conflicto con la Cuarta Enmienda. Además de estas restricciones, las mencionadas PET también deberían estar ampliamente al alcance de los individuos, para permitirles el anonimato en sus transacciones en red. Muchas empresas y grupos activistas están contribuyendo a difundir dichas tecnologías a través de Internet.

En este sentido, el anonimato significa simplemente «no rastreabilidad». Las herramientas que permiten este tipo de no rastreabilidad posibilitan que alguien envíe un mensaje sin que su contenido pueda acabar llevando hasta él, puesto que si se implementan adecuadamente dichas herramientas, no hay modo técnico de rastrear el mensaje. Esta clase de anonimato resulta esencial para determinadas formas de comunicación.

Estoy convencido de que, al menos mientras la represión política siga siendo una característica central de demasiados gobiernos mundiales, los gobiernos libres deberían garantizar por ley el derecho a estas tecnologías. Me hago cargo de lo controvertido de esta postura. Una menos extrema reconocería las diferencias entre el mundo digital y el real,[41] y garantizaría un derecho a comunicarse mediante seudónimos, pero no anónimamente. En este sentido, una transacción realizada con un seudónimo no puede relacionarse de forma obvia o directa con un individuo sin que intervenga un tribunal, pero contiene una huella dactilar efectiva que permitiría a la autoridad indicada, en las circunstancias oportunas, rastrear la comunicación hasta dar con su fuente.

41 Susan Brenner expresa esta idea de forma muy contundente, tal y como formula la pregunta: «¿Es razonable traducir los principios incluidos en la Cuarta Enmienda a un contexto creado y sustentado mediante la tecnología?». Susan Brenner, «The Privacy Privilege: Law Enforcement, Technology and the Constitution», *Journal of Technology Law and Policy*, núm. 7, 2002, pp. 123, 162. La cuestión no es simplemente si el anonimato tiene valor —sin duda lo tiene—, sino más bien «cómo traducir derechos concebidos para tratar con la conducta del mundo real a un mundo donde son posibles mayores grados de anonimato...», *ibidem*, pp. 139-140. «Dado que la tecnología altera los contornos del medio empírico donde se ejerce el derecho al anonimato, crea una tensión entre este aspecto del derecho a ser dejado en paz y las necesidades de aplicación efectiva de la ley», *ibidem*, p. 144.

En este régimen la cuestión importante es quién es la autoridad, y qué proceso se exige para acceder a la identificación. En mi opinión, la autoridad ha de ser el Estado, que debe someter su demanda de revelación de la identidad de un individuo a un proceso judicial, sin que el poder ejecutivo deba jamás disponer de la capacidad técnica para efectuar tal identificación por sí solo.

De nuevo, a nadie le agradará este equilibrio. Los amantes de la privacidad se enfurecerán ante cualquier respaldo a la vigilancia. Yo, en cambio, comparto la opinión del juez Posner de que una sofisticada tecnología de vigilancia podría realmente incrementar la privacidad efectiva si lograse reducir los casos en que los humanos se entrometen en las vidas ajenas. De modo similar, los amantes de la seguridad se mostrarán consternados ante la idea de que alguien abogue por tecnologías de anonimato. «¿Sabe usted lo complicado que es interceptar las comunicaciones electrónicas cifradas de un capo de la droga?», me preguntaron una vez.

Lo cierto es que no, no tengo una idea real al respecto. Pero también es cierto que promover la guerra contra las drogas me preocupa menos que permitir el florecimiento de la democracia. Las tecnologías que posibilitan este florecimiento también obstaculizarán aquella guerra o, para expresarlo de forma menos cobarde, las tecnologías que permiten que Aung San Suu Kyi siga luchando por la democracia en Birmania,[42] también permitirán que Al Qaeda continúe su guerra terrorista contra EEUU. Sí, lo admito. Y acepto que esto pueda conducir a otros a adoptar una postura menos extrema, pero urgiría a que el compromiso en favor de la vigilancia no sobrepase la protección que garantizan los seudónimos.

---

42 Aung San Suu Kyi es la figura más emblemática de la oposición birmana contra la dictadura militar que se perpetúa en el poder desde 1962. El partido opositor que ella dirige desde 1989, la Liga Nacional para la Democracia, llegó a ganar abrumadoramente las elecciones celebradas en 1990, pero la Junta Militar birmana no reconoció los resultados y le impidió formar gobierno. Galardonada con numerosos premios internacionales por su tarea de defensa de la democracia y los derechos humanos en Birmania (entre ellos el Premio Nobel de la Paz de 1991), Aung San Suu Kyi lleva los últimos diecinueve años bajo arresto domiciliario prácticamente ininterrumpido. [N. del E.]

Control de datos

El problema de controlar la difusión o el uso indebido de los datos es más complejo y ambiguo. Existen algunos usos de los datos personales ante los que muchos plantearían objeciones, pero muchos no equivale a todos. Hay quienes son totalmente felices revelando ciertos datos a entidades, y hay muchos más que lo serían si pudieran confiar en que sus datos se usan adecuadamente.

También en este caso, la solución pasa por una combinación de modalidades de regulación. Esta vez, sin embargo, empezaremos por la tecnología.[43]

Como describí exhaustivamente en el Capítulo 4, existe una presión emergente para incorporar una «capa de identidad» en Internet. A mi modo de ver, deberíamos considerar dicha capa de identidad como una PET: ésta permitiría que los individuos controlaran de modo más efectivo los datos personales que revelan; y también permitiría que los individuos dispusieran de una identidad seudónima fiable que tanto las páginas web como otras personas aceptaran encantadas. Así, mediante esta tecnología, si un sitio web necesita corroborar que soy mayor de edad, que tengo nacionalidad estadounidense o que estoy autorizado para acceder a una biblioteca universitaria, la tecnología certifique estos datos sin revelar nada más. De todos los cambios que podamos imaginar respecto a las prácticas informativas, éste sería el más trascendental a fin de reducir la cantidad de información redundante o innecesaria que fluye en el éter de la red.

Una segunda PET que posibilita un mayor control sobre el uso de los datos personales sería un protocolo denominado abreviadamente P3P (*Platform for Privacy Preferences*, Plataforma de Preferencias de Privacidad).[44]

---

43 Shawn C. Helms, «Translating Privacy Values with Technology», *Boston University Journal of Science and Technology Law*, núm. 7, 2001, pp. 288, 314. («Deberíamos enfocar la traducción del anonimato en Internet a través del "código", desarrollando e implementando tecnologías de aumento de la privacidad»).

44 Como escribe William McGeveran, Marc Rotenberg, uno de los más importantes defensores de la privacidad, no contempla la P3P como una PET «porque Rotenberg define la PET como una tecnología que reduce de forma inherente la transferencia de datos personales». William McGeveran, «Programmed Privacy Promises: P3P and Web Privacy Law», *New York University Law Review*, núm. 76, 2001, pp. 1813, 1826-1827, n. 80. Comparto la visión de McGeveran de que la P3P es una PET. Si la privacidad es el control sobre cómo se hace pública la información acerca de nosotros, entonces una tecnología que aumente ese control es una PET incluso si no «reduce [la] transferencia de datos personales» —siempre que dicha reducción sea coherente con las preferencias individuales. No cabe duda de que una PET puede ser una mala PET en la medida en que no llegue a

La P3P permitiría una expresión de las preferencias de privacidad de un individuo que las máquinas pueden leer, propiciando de forma automática que el individuo reconozca cuándo un sitio no cumple con sus preferencias de privacidad. Así, si accedemos a un sitio que expresa su política de privacidad mediante P3P, y dicha política es incoherente con nuestras preferencias, entonces, dependiendo de la implementación, o bien el sitio, o bien nosotros, recibimos una advertencia del problema creado por este conflicto. De este modo, la tecnología podría revelar que existe ese conflicto, y reconocerlo es el primer paso para proteger nuestras preferencias.

La parte crucial de esta estrategia es conseguir que estas opciones sean legibles por máquinas. Si buscamos en Google «política de privacidad», aparecerá casi un cuarto de billón de referencias en la red, y si consultamos la amplia mayoría de ellas (cosa que no podríamos hacer en esta vida), daremos con textos legales que están entre los más incomprensibles que se pueden encontrar (que ya es decir). Estas políticas son producto del pensamiento pre-internet acerca de cómo abordar problemas de esta naturaleza. Así, cuando se presionó al gobierno para que «solucionara» el problema de la privacidad en Internet, su solución consistió en exigir que se publicaran «políticas de privacidad» por doquier. Ahora bien, ¿alguien se las lee realmente? Y si alguien lo hace, ¿acaso las recuerda al pasar de un sitio a otro? ¿Conoce el lector la diferencia entre la política de privacidad de Amazon y la de Google?

El error del gobierno fue no exigir que dichas políticas también fueran comprensibles por los ordenadores. Porque si tuviéramos un cuarto de billón de sitios con declaraciones de política de privacidad legibles tanto por humanos como por máquinas, entonces dispondríamos de la infraestructura necesaria para fomentar el desarrollo de esta PET, la P3P. Pero como el gobierno no pudo pensar más allá de su tradicional manera de legislar —como no se le ocurrió exigir cambios en el código además de textos legales—, ahora no contamos con esa infraestructura. Sea como fuere, mi visión es que tal exigencia es crucial.

Con todo, estas tecnologías por sí solas no pueden hacer nada para solucionar el problema de la privacidad en la Red. Está meridianamente claro que, para complementarlas, necesitamos la regulación legal; ésta puede ser

permitir la elección, pero no lo es por impedir la elección de todo aquél que no sea el consumidor. Para un relato maravilloso de cómo las normas se han erigido en artífices del cambio en las prácticas de privacidad de datos, véase Steven A. Hetcher, «Norm Proselytizers Create a Privacy Entitlement in Cyberspace», *Berkeley Technology Law Journal*, núm. 16, 2001, p. 877.

de tres clases diferentes. La primera es sustantiva —leyes que establecen los límites de la protección de la privacidad– la segunda es procedimental —leyes que imponen procedimientos justos para abordar las prácticas de privacidad– y la tercera es habilitante —leyes que velan por el cumplimiento de los acuerdos de respeto de la privacidad suscritos entre individuos y empresas.

1. Límites de elección

Una clase de legislación está diseñada para limitar la libertad individual. Del mismo modo que la legislación laboral prohíbe ciertos contratos de trabajo, o que la legislación de los consumidores veta determinados acuerdos de crédito, esta clase de legislación de privacidad restringiría la libertad individual de revelar ciertos aspectos de su vida privada. El motivo de esta limitación podría ser sustantivo o procedimental —sustantivo en cuanto que refleja un juicio sustantivo acerca de opciones que los individuos no deberían elegir; o procedimental en cuanto que refleja la opinión de que, al enfrentarse a esta elección, los individuos elegirán sistemáticamente de tal modo que luego se lamentarán. En uno u otro caso, el papel de este tipo de regulación de privacidad es bloquear las transacciones susceptibles de debilitar la privacidad en el seno de una comunidad.

2. El proceso para proteger la privacidad

La estructura normativa más importante relacionada con las prácticas de privacidad fue establecida hace más de treinta años por el comité asesor en sistemas automatizados de datos del Departamento de Salud, Educación y Bienestar de EEUU. El informe de este comité asesor señaló cinco principios que definen el «Código de buenas prácticas de información».[45] Estos principios plantean los siguientes requisitos:

---

45 Véase US Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, viii, 1973, citado en http://www.epic.org/privacy/consumer/code_fair_info.html.

1. No debe haber ningún sistema de conservación de registros de datos personales cuya existencia sea secreta.

2. Las personas deben disponer de un modo de averiguar qué información acerca de ellas está incluida en un registro y cómo es usada.

3. Las personas deben disponer de un modo de impedir que la información acerca de ellas que se obtuvo con un fin determinado sea usada o se haga disponible con otros fines sin su consentimiento.

4. Las personas deben disponer de un modo de corregir o rectificar un registro de información identificable acerca de ellas.

5. Cualquier organización que se dedique a crear, mantener, usar o diseminar registros de datos personales identificables debe asegurar la fiabilidad de los datos para su uso previsto y debe tomar precauciones para impedir el uso indebido de dichos datos.

Estos principios expresan importantes valores sustantivos —por ejemplo, que los datos no se reutilicen más allá de un consentimiento original, o que los sistemas de recopilación sean fiables—, pero no interfieren con la opción individual de alguien de revelar sus datos personales con fines concretos. En este sentido, son principios que aumentan la autonomía individual, y cuyo espíritu ha guiado el abanico relativamente estrecho y *ad hoc* de la legislación de privacidad que se ha promulgado tanto en EEUU en general como en sus diferentes estados.[46]

3. Reglas para permitir opciones de privacidad

El auténtico desafío para la privacidad, sin embargo, es cómo permitir una elección significativa en la era digital. Y a este respecto, la técnica que el gobierno estadounidense ha empleado hasta ahora —a saber, la exigencia de declaraciones de política de privacidad basadas en texto— es un ejemplo perfecto de cómo *no* actuar. Atiborrar la Red de palabras incomprensibles no potenciará que los consumidores realicen elecciones útiles al navegar por Internet; en todo caso, les ahuyentará de intentar siquiera comprender a qué derechos renuncian cuando se mueven de un sitio a otro.

46 *Ibidem*.

La P3P sería de ayuda a este respecto, pero sólo si (1) hubiera un decidido impulso para difundir la tecnología a través de las áreas de la red, y (2) las representaciones realizadas dentro de la infraestructura P3P fueran aplicables. Y para que ambas condiciones sean efectivas es necesaria la acción de la ley.

En la primera edición de este libro, propuse una estrategia que, a mi modo de ver, cumpliría ambas condiciones: a saber, protegiendo los datos personales mediante un derecho de propiedad. Como sucede con el copyright, un derecho de propiedad sobre la privacidad proporcionaría poderosos incentivos a quienes desean usar esa propiedad para garantizar el consentimiento oportuno, el cual podría entonces encauzarse (a través de leyes) mediante las tecnologías adecuadas. Ahora bien, sin dicho consentimiento, el usuario de esa propiedad *privada* sería un pirata de la privacidad. De hecho, muchas de las mismas herramientas que podrían proteger el copyright en este sentido podrían también usarse para proteger la privacidad.

Esta solución también reconoce la que considero que es una característica importante de la privacidad —el hecho de que la gente la valora de forma diferente—,[47] y respeta asimismo esas diferentes valoraciones. Quizá para mí sea extremadamente importante que mi número de teléfono no sea fácilmente accesible, pero puede que al lector eso le traiga sin cuidado. Y como la presunta preferencia de la ley es la de usar un dispositivo legal que proporcione a los individuos la libertad de ser diferentes —es decir, la libertad de tener valores subjetivos completamente diferentes, y de que sean respetados—, ello sugiere que el dispositivo que utilicemos aquí sea la propiedad. Un sistema de propiedad está diseñado precisamente para permitir que las diferencias de valores sean respetadas por la ley. Así, si alguien decide no vender su flamante Chevy Nova por menos de diez mil dólares, la ley le respaldará.

El beneficio legal opuesto en la tradición jurídica estadounidense es la denominada «regla de responsabilidad».[48] Una regla de responsabilidad también protege un beneficio, pero su protección es menos individual.

---

47 Lior Jacob Strahilevitz explora de forma aguda esta cuestión fundamentalmente «empírica» en «A Social Networks Theory of Privacy», *University of Chicago Law Review*, núm. 72, 2005, pp. 919, 921.

48 Véase Guido Calabresi y A. Douglas Melamed, «Property Rules, Liability Rules, and Inalienability: One View of the Cathedral», *Harvard Law Review*, núm. 85, 1972, pp. 1089, 1105-1106. «Las reglas de propiedad implican una decisión colectiva acerca de a quién ha de concederse un beneficio inicial, pero no acerca del valor de dicho beneficio. [...] Las reglas de responsabilidad implican una fase adicional de intervención estatal: no sólo se protegen los beneficios, sino que su transferencia o destrucción son permitidas sobre la base de un valor determinado por algún órgano estatal, en lugar de por las propias partes» (p. 1092).

Si alguien posee un recurso protegido por una regla de responsabilidad, yo puedo tomarlo con tal de que pague un precio fijado por el Estado. Este precio puede ser mayor o menor del que su poseedor establezca, pero lo importante es que, independientemente de ello, tengo todo el derecho a tomar ese recurso.

Un ejemplo proveniente de la ley de propiedad intelectual puede dejar esta idea más clara. El derecho de transformación es el derecho a realizar una obra derivada a partir de un contenido bajo copyright. Un ejemplo tradicional de obra derivada sería una traducción o una película basada en un libro. La ley de propiedad intelectual concede al titular de los derechos de autor un derecho de propiedad sobre ese derecho de transformación. Por lo tanto, si alguien desea adaptar al cine la última novela de John Grisham, ha de pagarle lo que éste le pida; si no lo hace y rueda la película, habrá violado los derechos de Grisham.

Eso mismo no ocurre con los derechos de transformación de los compositores de música.[49] Si un compositor autoriza a alguien a grabar una canción suya, entonces cualquier otro tiene derecho a grabar esa misma canción, siempre y cuando siga ciertos procedimientos y pague la tasa especificada. Por lo tanto, mientras que Grisham puede optar por conceder a un solo cineasta el derecho a hacer una película basada en su novela, los Beatles han de permitir que cualquiera grabe una canción compuesta por uno de los miembros del grupo, con tal de que les pague por ello. El derecho de transformación de novelas está protegido, pues, por una regla de propiedad, mientras que el derecho de transformación de fonogramas lo está por una regla de responsabilidad.

La ley tiene toda clase de razones para imponer una regla de responsabilidad en lugar de una de propiedad. Ahora bien, el principio general es que deberíamos usar una regla de propiedad, al menos allí donde los «costes de transacción» de negociar sean bajos y no exista un principio público contradictorio.[50] Y mi visión es que, con una tecnología como la P3P, podríamos reducir los costes de transacción lo bastante como para que funcionara una regla de propiedad. Y esta regla, a su vez, reforzaría la diversidad de perspectivas que la gente tiene sobre su privacidad —permitiendo a algunos renunciar a sus derechos y a otros afianzarlos.

---

49 El autor desarrolla a partir de aquí su ejemplo basándose en cláusulas específicas de la legislación estadounidense. [N. del E.]

50 *Ibidem*.

Y había una razón adicional por la que defendí un derecho de propiedad para la protección de la privacidad. A mi juicio, dicha protección sería más sólida si la gente concibiera el derecho a la privacidad como un derecho de propiedad. La gente necesita apoderarse de este derecho y protegerlo, y la propiedad es la herramienta tradicional que usamos para identificar y permitir la protección. Si pudiéramos ver una fracción de la pasión con la que se defiende actualmente el copyright en la defensa de la privacidad, puede que progresáramos en su protección.

No obstante, mi propuesta de un derecho de propiedad fue rechazada sonadamente con críticas cuyos puntos de vista respeto.[51] No estoy de acuerdo con el núcleo de estas críticas y, por las razones puestas en orden de manera contundente por Neil Richards, discrepo especialmente de la afirmación según la cual el derecho de propiedad sobre la privacidad provocaría un problema con la Primera Enmienda.[52] En cualquier caso, William McGeveran sugirió una alternativa que alcanzaba el mismo objetivo que yo buscaba sin suscitar ninguna de las preocupaciones que más espolearon a los críticos.[53]

Tal alternativa simplemente especifica que una representación realizada por un sitio web mediante el protocolo P3P se considera una oferta vinculante que, en caso de ser aceptada por quien accede al sitio, se convierte en un contrato ejecutable.[54] Esa regla, ligada al requisito de que las políticas de privacidad se expresen de una forma legible por máquinas, como la P3P,

---

51 Véase, por ejemplo, Mark A. Lemley, «Private Property», *Stanford Law Review*, núm. 52, 2000, pp. 1545, 1547; Paul M. Schwartz, «Beyond Lessig's Code for Internet Privacy: Cyberspace Filter, Privacy Control, and Fair Information Practices», *Wisconsin Law Review*, 2000, p. 743; Julie E. Cohen, «DRM and Privacy», *Berkeley Technology Law Journal*, núm. 18, 2003, pp. 575, 577; Marc Rotenberg, «Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)», *Stanford Technology Law Review*, 2001, pp. 1, 89-90. Andrew Shapiro discute una idea similar en *The Control Revolution*, *op. cit.*, pp. 158-165.

52 Véase Neil M. Richards, «Reconciling Data Privacy and the First Amendment» *UCLA Law Review*, núm. 52, 2005, pp. 1148, 116. Richards identifica correctamente al brillante Eugene Volokh como el defensor más enérgico de la idea de que la Primera Enmienda restringe la propiedad de la privacidad. Pero la visión exhaustiva que ofrece Richards del abanico de reglas que regulan la privacidad resulta bastante persuasiva contra la postura de Volokh.

53 William McGeveran, «Programmed Privacy Promises: P3P and Web Privacy Law», *New York University Law Review*, núm. 76, 2001, pp. 1813, 1843.

54 El importante límite de los contratos, no obstante, es que, típicamente, éstos vinculan sólo a los implicados en el acuerdo bipartito (*within privity*), es decir, a las partes del contrato. Por consiguiente, el acuerdo que yo establezco con el lector por el que éste promete no usar un libro que le he vendido (por ejemplo, su promesa de no publicar una reseña del libro antes de cierta fecha) no vinculará a otra persona que encuentre casualmente el libro y lo lea.

contribuiría tanto a (1) difundir la P3P como a (2) sancionar legalmente las aseveraciones de la P3P. Esto seguiría siendo más débil que una regla de propiedad, por razones que dejaré para las notas,[55] y puede fomentar en buena medida la cultura de los contratos de adhesión, que ocasionan sus propios problemas, pero de acuerdo con mi propósito aquí, esta solución supone un útil compromiso.

Para ilustrar nuevamente la dinámica del ciberderecho: empleamos la ley (un requisito de políticas de privacidad expresadas de una forma determinada, y una presunción contractual acerca de dichas expresiones) para fomentar cierta clase de tecnología (la P3P), de modo que ella permita que en el ciberespacio los individuos puedan lograr más fácilmente lo que desean. Se trata, pues, de la *ley* ayudando al *código* a perfeccionar la *política* de privacidad.

Ello no equivale a afirmar, por descontado, que no disponemos de protecciones para la privacidad. Como hemos analizado en profundidad, hay más leyes aparte de las federales y más reguladores aparte de la ley. A veces estos otros reguladores pueden proteger la privacidad mejor de lo que lo hace la ley, pero cuando no sea así, mi postura es que la ley es necesaria.

Privacidad comparada

Es probable que el lector insatisfecho con el argumento que sostuve en el capítulo anterior comience a formular preguntas mordaces: «¿Acaso no rechazó usted en el capítulo anterior justo el mismo régimen que está respaldando en éste? ¿No rechazó usted una arquitectura que facilitara la venta perfecta de propiedad intelectual? ¿No es precisamente eso lo que ha creado usted aquí?».

La acusación que se me imputa es bastante certera. He respaldado una arquitectura que es esencialmente la misma que cuestioné con respecto a la propiedad intelectual. Ambas constituyen regímenes para el intercambio de

55 Como describí en la nota anterior, tal debilidad está relacionada con la idea expuesta acerca de la vinculación contractual bipartita. A diferencia de una regla de propiedad, que viaja automáticamente con la propiedad, una regla construida a partir de acuerdos alcanza exclusivamente hasta donde alcanzan dichos acuerdos.

información y tratan la información «como» una propiedad «real». Pero con respecto a la propiedad intelectual, impugné un régimen de propiedad completamente privatizado; y con respecto a la privacidad, lo estoy defendiendo. ¿En qué quedamos?

La diferencia radica en los principios subyacentes que dan forma sustancial, o deberían hacerlo, a la información en cada contexto. En el contexto de la propiedad intelectual, deberíamos inclinarnos por la libertad. Nadie sabe a ciencia cierta qué es lo que «la información quiere»,[56] pero sea lo que sea, deberíamos interpretar el acuerdo al que la ley llega con los titulares de derechos de autor de la forma más restrictiva posible. Deberíamos mantener una actitud reticente ante los derechos de propiedad con respecto a la propiedad intelectual, y apoyarlos exclusivamente en la medida en que sean necesarios para construir y sustentar regímenes de información.

Ahora bien, la información personal (al menos algunos tipos de ella) debería tratarse de forma diferente. Nadie llega a un acuerdo con la ley con respecto a la información personal o privada; y la ley no nos ofrece un derecho de monopolio a cambio de que publiquemos esta información. He aquí lo que distingue la privacidad de la propiedad intelectual: que los individuos deberían estar capacitados para controlar la información sobre sí mismos. Deberíamos estar ávidos por ayudarles a proteger esa información, proporcionándoles las estructuras y los derechos para hacerlo. Todos valoramos, o deseamos, nuestra paz. Y por lo tanto, un régimen que nos facilita esa paz, otorgándonos el control sobre la información privada, es un régimen coherente con los valores públicos que las autoridades públicas deberían respaldar.

---

56 Barlow, «The Economy of Ideas», *Wired*, marzo de 1994, disponible en http://www. wired.com/wired/archive/2.03/economy.ideas.html (*information wants be free*, «la información quiere ser libre»).

[Esta célebre divisa a la que alude el autor, *Information wants to be free*, fue formulada originalmente por el mencionado Stewart Brand (concretamente en la página 202 de *The Media Lab: Inventing the Future at MIT*, Viking Penguin Press, Nueva York, 1987) y posee una coletilla que juega con el doble sentido del adjetivo inglés *free* como «libre» y como «gratis». Lo significativo de esta coletilla y el hecho de que se la omita de forma impenitente en la mayoría de ocasiones en que se cita hacen que juzgue relevante incluir aquí mi traducción del fragmento donde ésta se inserta:

> La información quiere ser libre. La información también quiere ser cara. La información quiere ser libre porque se ha vuelto muy barata de distribuir, copiar y recombinar —demasiado barata para medirla [*too cheap to meter* —eslogan propagandístico de la industria nuclear]. Y quiere ser cara porque puede poseer un valor incalculable para su receptor. Esa tensión no desaparecerá (p. 202).

N. del E.]

Hay un segundo modo, acaso más favorable, de defender esta misma idea. La propiedad intelectual, una vez creada, no constituye un bien rival: cuanta más gente la usa, más beneficiada se ve la sociedad. Por eso nos inclinamos por la compartición y la libertad en el contexto de la propiedad intelectual. La privacidad, por el contrario, sí que se gasta con el uso: cuanta más gente esté autorizada a pisotearla, menos quedará de ella. En este sentido, la privacidad se asemeja más a la propiedad real que a la intelectual. Ninguna intrusión individual puede llegar a destruirla, pero su valor se reduce en cierta medida con cada nueva invasión.

Esta conclusión está sujeta a importantes matizaciones, dos de las cuales describo a continuación.

La primera es que no hay nada en el régimen que propongo que conceda a los individuos un control definitivo o absoluto sobre los tipos de datos que pueden vender o los tipos de privacidad que pueden comprar. El régimen basado en la P3P permitiría, en principio, tanto un control de los derechos de privacidad en los niveles superiores como otro individual. Si, por ejemplo, viviéramos en un régimen que identificase a los individuos según su jurisdicción, entonces las transacciones en el seno del régimen basado en la P3P podrían limitarse en función de las reglas de las jurisdicciones específicas.

La segunda es que no hay razón para que tal régimen tenga que proteger todos los tipos de datos privados, y nada en el esquema planteado hasta ahora nos indica qué debería considerarse información «privada» y qué no. Puede haber hechos acerca de nosotros mismos que no se nos permita ocultar; y más importante aún, puede haber afirmaciones acerca de nosotros mismos que no se nos permita formular («soy abogado» o «llámeme, soy médico»). No debería permitirse que incurriéramos en fraude o que perjudicáramos a los demás. Esta limitación es análoga al «uso justo» de la propiedad intelectual —un límite al espacio que puede proteger la privacidad.

Comencé el presente capítulo afirmando que, por lo que se refiere a la privacidad, ya se ha levantado la liebre. Y es que ya tenemos arquitecturas que deniegan a los individuos el control sobre lo que otros saben sobre ellos; la cuestión es qué podemos hacer en respuesta a ello.

Mi respuesta ha sido: «mira el código, Luke». Hemos de integrar en la arquitectura una capacidad que posibilite la elección —una elección hecha por máquinas, y no por humanos. La arquitectura debe permitir las negociaciones sobre privacidad entre máquinas de modo que los individuos puedan dar instrucciones a sus máquinas acerca del grado de privacidad que desean proteger.

Pero, ¿cómo llegaremos a eso? ¿Cómo puede erigirse esa arquitectura? Los individuos pueden querer que el ciberespacio proteja su privacidad, pero ¿qué empujará al ciberespacio a incorporar las arquitecturas necesarias?

El mercado, no; el poder del comercio no estará detrás de una transformación así. A este respecto, la mano invisible sería realmente invisible. Debe emprenderse, pues, una acción colectiva para empujar las arquitecturas hacia este objetivo, y la política está precisamente para ocuparse de la acción colectiva. El *laissez-faire* no solucionará nada.

12. Libertad de expresión

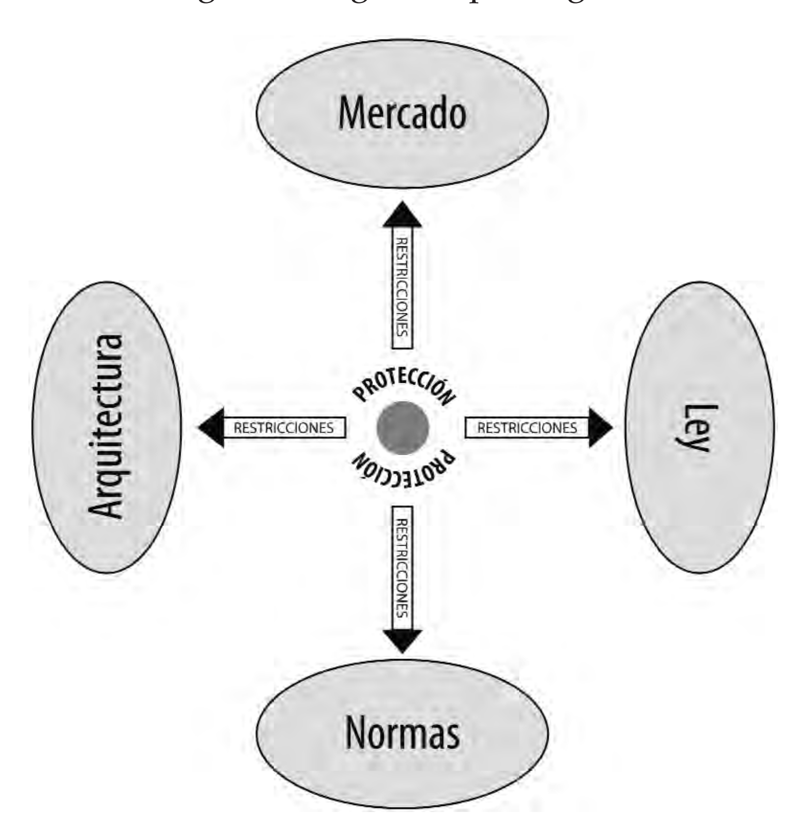
El derecho a la libertad de expresión no equivale al derecho a expresarse gratis; y tampoco al derecho de acceso gratuito a la televisión, o al derecho a que la gente no nos odie por lo que tenemos que decir. En términos estrictos —y en términos legales—, el derecho a la libertad de expresión en EEUU es el derecho a no ser castigado por el Estado como represalia por casi nada de lo que se diga. Nadie puede ser encarcelado por criticar al Presidente, aunque sí por amenazarle; nadie puede ser multado por promover la segregación, aunque muchos le volverán la espalda si lo hace. A nadie se le puede impedir hablar en un espacio público, aunque sí se le puede impedir hacerlo con un transmisor FM. En EEUU, la libertad de expresión está protegida —de un modo complejo, y a veces enrevesado—, pero su protección constitucional constituye una protección contra el Estado.

No obstante, una explicación constitucional de la libertad de expresión que sólo considerase al Estado sería radicalmente incompleta. Dos sociedades distintas podrían tener la misma «Primera Enmienda» —las mismas protecciones contra la cólera del Estado— pero si en una se tolera a los disidentes y en otra se los rechaza, estaríamos ante dos sociedades con libertades de expresión muy diferentes. Las restricciones a la expresión van más allá del Estado, y lo mismo ocurre con sus protecciones. Una explicación completa de este —y de cualquier— derecho ha de considerar el repertorio total de gravámenes y protecciones que le atañen.

Consideremos, por ejemplo, los «derechos» de las personas con discapacidad con respecto a la protección contra la discriminación, tal y como quedan construidos por las cuatro modalidades del Capítulo 7. La ley protege a las personas con discapacidad; no así las normas sociales;

el mercado proporciona bienes para ayudarles, pero sobre ellas recae todo el coste de su adquisición; y hasta que la ley intervino, la arquitectura contribuyó bien poco a integrar a las personas con discapacidad en la sociedad (sólo hay que pensar en las escaleras). El remanente resultante de estas cuatro modalidades describe la protección, o los «derechos», que tienen las personas con discapacidad en cualquier contexto concreto. La ley puede intervenir para reforzar esa protección —por ejemplo, regulando la arquitectura para que integre mejor a esas personas—, pero para cualquier «derecho» dado, podemos usar esta combinación de modalidades para describir lo bien (o mal) que está protegido.

En los términos del Capítulo 7, estamos, pues, ante modalidades tanto de regulación como de protección. Es decir, dichas modalidades pueden funcionar como restricciones a la conducta y también como protecciones contra otras restricciones. La siguiente figura captura gráficamente esta idea.



En el centro de la figura está el objeto regulado —el pobre punto del Capítulo 7. Rodeando al individuo aparece ahora un escudo de protección, una combinación de leyes, normas, mercado y arquitectura que limita las restricciones que esas mismas modalidades impondrían sobre el individuo de otro modo. No he separado las cuatro en la esfera del escudo porque obviamente no existe una correspondencia directa entre la modalidad de restricción y la de protección. Cuando la ley como protección entra en conflicto con la ley como restricción, la ley constitucional prevalece sobre la ley ordinaria.

Dichas modalidades funcionan conjuntamente. Puede que unas socaven a otras, lo que implica que la suma de las protecciones podría parecer menos significativa que la suma de las partes. El «derecho» a promover la despenalización de las drogas en el actual contexto de la llamada «guerra contra las drogas» constituye un ejemplo de ello. La ley protege nuestro derecho a abogar por la despenalización de las drogas. El Estado no puede encerrarnos si, como George Soros, lanzamos una campaña para la despenalización de la marihuana, o si, como el Premio Nobel de Economía Milton Friedman o el juez federal Richard Posner, escribimos artículos sugiriendo esa idea. Si algo significa la Primera Enmienda, es precisamente que el Estado no puede criminalizar la expresión acerca de reformas legales.

Ahora bien, esa protección legal no significa que mi promoción de la despenalización de las drogas vaya a carecer de consecuencias. Mis vecinos se sentirán horrorizados ante la idea, y algunos, sin duda, me rechazarían. El mercado tampoco me apoyaría necesariamente: en la práctica, resulta imposible comprar franjas publicitarias televisivas para abogar por tal reforma. Las cadenas de televisión tienen derecho a seleccionar sus anuncios (dentro de unos límites), y lo más probable es que juzgaran los míos como demasiado controvertidos.[1] Además, dichas cadenas se encuentran bajo la supervisión de la Comisión Federal de Comunicaciones (FCC) —un activo combatiente en la guerra contra las drogas. E incluso si se me permitiera emitir mis anuncios, yo no soy George Soros y no dispongo de millones de dólares para invertir en esta campaña. Puede que consiguiera insertar algún anuncio en una televisión local a horas intempestivas, pero no podría permitirme, por ejemplo, una campaña televisiva nacional en horario de máxima audiencia.

Finalmente, la arquitectura tampoco protegería mi derecho de expresión demasiado bien. Y es que, en EEUU al menos, existen pocos sitios donde uno pueda situarse frente a una audiencia y dirigirse a ella para abordar algún asunto de relevancia pública sin que la mayoría lo tilde de chiflado o latoso. No existe un *Speakers' Corner* en cada ciudad; de hecho, la mayoría de las ciudades estadounidenses no celebra el tradicional *town meeting*, reuniones municipales anuales donde todos los ciudadanos se congregan para debatir y tomar decisiones en materia de política local. En este sentido, la «América *offline*» se asemeja mucho a America Online, puesto que no está diseñada para permitir que los individuos se dirijan a una amplia audiencia

---

1 Véase 47 CFR 73.658(e), 1998; véase también Herbert J. Rotfeld *et al*., «Television Station Standards for Acceptable Advertising», *Journal of Consumer Affairs*, núm. 24, 1990, p. 392.

para abordar asuntos de interés público. Esto queda reservado para los profesionales —políticos, eruditos, famosos, periodistas y activistas, la mayoría de los cuales se ciñe a un asunto particular—, mientras que al resto de ciudadanos se les plantea una disyuntiva: o bien escuchar, o bien ser despachados al *gulag* de los lunáticos sociales.

Por consiguiente, la protección en la práctica de un enunciado controvertido es más condicional de lo que sugeriría un punto de vista exclusivamente legal. O dicho de otro modo, al tomar en consideración algo más que la ley, el derecho a ser un disidente está menos protegido de lo que podría.

Traslademos ahora este ejemplo al ciberespacio. ¿Cómo está protegido allí el «derecho» a promover la despenalización de las drogas? En el ciberespacio, por supuesto, la ley también protege mi derecho a abogar por esa medida —al menos en EEUU. No obstante, es bastante posible que mi expresión sea ilegal en otros lugares y que puedan procesarme por lanzar esas ideas al ciberespacio «en» otro país. Así por ejemplo, la propaganda del Partido Nazi es legal en EEUU, pero no así en Alemania,[2] con lo que su difusión en el ciberespacio también puede acarrear responsabilidades penales en el espacio alemán.

La ley constituye, por lo tanto, una protección imperfecta. ¿Contribuyen las normas a proteger la expresión en el ciberespacio? Con el relativo anonimato del ciberespacio y su creciente expansión, las normas tampoco funcionan bien allí. Incluso en ciberespacios donde la gente se conoce bien, es probable que se sea más tolerante con las ideas disidentes cuando se sabe (o se cree, o se espera) que quien las defiende vive a miles de kilómetros.

El mercado también proporciona una protección mayor a la expresión en el ciberespacio; comparadas con las del espacio real, las restricciones que el mercado impone a la expresión en el ciberespacio son mínimas. Recordemos con qué facilidad Jake Baker se convirtió en un editor con una audiencia potencial mucho mayor que la de todos los libros de derecho publicados en la última década (incluido éste). Fijémonos en los más de 50 millones de *blogs* que actualmente permiten a millones de personas expresar sus opiniones

---

2 Véase el *Strafgesetzbuch* (StGB, Código Penal alemán), pp. 130–131, reimpreso en Gerold Harfst (ed.), *German Criminal Law,* vol. 1, trad. por Otto A. Schmidt, Würzburg, Harfst Verlag, 1989, pp. 75–76 [ed. cast: Emilio Eiranova Encinas (coord.), *Código Penal Alemán StGB, Código Procesal Penal Alemán StPO*, trad. por Juan Ortiz de Noriega, Madrid, Marcial Pons, 2000].

acerca de cualquier asunto. El bajo coste de la edición conlleva que ésta deje de ser una barrera para la expresión. Tal y como pregunta Eben Moglen: «¿Existirá algún poeta inédito en el siglo XXI?».

Con todo, la modalidad que encabeza esta lista de protectores de la expresión en el ciberespacio es (una vez más) la arquitectura. Anonimato relativo, distribución descentralizada, múltiples puntos de acceso, ausencia de necesidad de ataduras geográficas, inexistencia de un sistema simple para identificar contenidos, herramientas criptográficas—[3] todos estos atributos y consecuencias del protocolo de Internet dificultan el control de la expresión en el ciberespacio. La arquitectura del ciberespacio es la verdadera protectora de la expresión; constituye la «Primera Enmienda en el ciberespacio», y esta Primera Enmienda ya no es ninguna ordenanza local.[4]

Detengámonos a pensar en lo que esto significa. Durante más de sesenta años, EEUU ha sido exportador de una determinada ideología política en cuyo núcleo se halla una determinada concepción de la libertad de expresión. Muchos han criticado esta concepción: algunos la encuentran demasiado extrema y otros no lo suficiente. Los regímenes represivos —China, Corea del Norte— la rechazaron directamente; los regímenes tolerantes —Francia, Hungría— se quejaron de la decadencia cultural que propicia; los regímenes igualitarios —los países escandinavos— no se explicaban cómo los estadounidenses podíamos considerarnos libres cuando sólo los ricos pueden hablar y la pornografía está reprimida.

---

3 Construidas por la industria pero también especialmente por los *Cypherpunks* —escritores de código dedicados a construir las herramientas de la privacidad para Internet. Como escribe Eric Hughes en «A Cypherpunk's Manifesto», en Bruce Schneier (ed.), *Applied Cryptography,* (2ª), Nueva York, Wiley, 1996, p. 609: «Nosotros, los *Cypherpunks*, nos dedicamos a construir sistemas anónimos. Defendemos nuestra privacidad por medio de la criptografía, de sistemas anónimos de reenvío de correo electrónico y de dinero electrónico. Los *Cypherpunks* escribimos código. Somos conscientes de que alguien tiene que escribir el software que defienda la privacidad, y como no la podremos alcanzar si no ponemos todos de nuestra parte, vamos a hacerlo nosotros. Publicamos nuestro código de modo que nuestros compañeros *Cypherpunks* puedan practicar y jugar con él. Cualquiera es libre de usar nuestro código en cualquier parte del mundo» [ed. cast.: «Un Manifiesto Cripto-hacker» en Carlos Gradin (comp.), *Internet, hackers y software libre*, Buenos Aires, Editora Fantasma, 2004, pp. 95-99; disponible en www.dyne.org/editora_fantasma.pdf].

4 John Perry Barlow ha puesto en circulación el *meme* [unidad de información cultural que se transmite de una mente a otra, según la teoría del investigador británico Richard Dawkins] «en el ciberespacio, la Primera Enmienda es una ordenanza local»; «Leaving the Physical World», disponible en http://www.eff.org/Misc/Publications/John_Perry_Barlow/HTML/leaving_the_physical_world.html.

Este debate se ha prolongado en el plano político durante mucho tiempo y, sin embargo, como resguardados por cierta nocturnidad, ahora hemos conectado estas naciones mediante una arquitectura de comunicación que construye dentro de sus fronteras una Primera Enmienda mucho más potente que cualquiera que nuestra ideología haya promovido jamás. Un buen día las naciones se despiertan y descubren que sus líneas telefónicas son herramientas de libertad de expresión, que los correos electrónicos expanden noticias de su represión mucho más allá de sus fronteras, que las imágenes dejan de estar monopolizadas por las cadenas de televisión estatales y pueden transmitirse ahora desde un simple módem. Así pues, hemos exportado al mundo, a través de la arquitectura de Internet, una Primera Enmienda en forma de código más radical que nuestra propia Primera Enmienda en forma de ley.

Este capítulo trata de la regulación de la expresión y de su protección en el ciberespacio —y, en consecuencia, también en el espacio real. Mi objetivo es destacar la relación entre la arquitectura y la libertad que ésta hace posible, así como la importancia de la ley en la construcción de esa arquitectura. Con esto pretendo que el lector comprenda cómo está edificada esta libertad —la política constitucional en la arquitectura del ciberespacio.

Y digo «política» porque dicha edificación no ha acabado. Tal y como vengo defendiendo (una y otra vez), no existe una única arquitectura para el ciberespacio, ni tampoco una estructura dada o necesaria en su diseño. Puede que la Internet de primera generación haya abierto grietas en los muros de control, pero no hay razón para creer que los arquitectos de segunda generación harán lo mismo, o para no esperar que una segunda generación reconstruya el control resquebrajado. En otras palabras, no hay razón para pensar que este fogonazo inicial de libertad no tenga los días contados; y ciertamente tampoco hay justificación para actuar como si no fuera a ser así.

Ya podemos vislumbrar los inicios de la reconstrucción mencionada. Se están rehaciendo las arquitecturas para volver a regular lo que la arquitectura del espacio real hacía regulable anteriormente. La Red ya está pasando de ser libre a ser controlada.

Algunos de estos pasos hacia la restauración de la regulación son inevitables; hay pasos que no admiten vuelta atrás. Sin embargo, antes de que el cambio sea completo, debemos comprender las libertades que la Red proporciona en este momento y determinar cuáles de ellas queremos preservar.

Y no sólo preservar. La arquitectura de Internet, tal y como es ahora mismo, constituye quizá el modelo más importante de libertad de expresión desde la fundación de EEUU, con implicaciones que van más allá del correo electrónico y las páginas web. Doscientos años después de que sus redactores ratificasen la Constitución, la Red nos ha enseñado el verdadero significado de la Primera Enmienda. Si tomamos en serio dicho significado, la Primera Enmienda nos exigirá una reestructuración bastante radical de las arquitecturas de expresión también fuera de la red.[5]

Pero estoy adelantándome a la historia. En lo que queda de este capítulo, trataré cuatro cuestiones distintas acerca de la libertad de expresión en el ciberespacio. Con cada una de ellas, deseo examinar como es regulada dicha «libertad de expresión».

Estas historias no tienen todas la misma importancia constitucional, pero todas ellas ilustran la dinámica que se encuentra en el núcleo de la argumentación que presento en este libro —cómo la arquitectura interactúa con la ley para determinar las políticas.

Los reguladores de la expresión: publicación

Floyd Abrams es uno de los abogados especialistas en libertad de expresión más conocido de EEUU. En 1971 era un joven socio del bufete Cahill Gordon.[6] A última hora de la tarde del lunes 14 de junio de ese año, Abrams recibió una llamada de James Goodale, abogado de *The New York Times*. Éste le pidió que, junto a Alexander Bickel, profesor de la Facultad de Derecho de Yale, defendiera a su periódico en una demanda que se iba a interponer contra él al día siguiente.

---

5 O puede que nuestra interpretación de la doctrina de la Primera Enmienda no se centre lo suficiente en su historia con relación a los medios electrónicos. Véase Marvin Ammori, «Another Worthy Tradition: How the Free Speech Curriculum Ignores Electronic Media and Distorts Free Speech Doctrine», *Missouri Law Review*, núm. 70, 2005, p. 59.

6 Véase David Rudenstine, *The Day the Presses Stopped: A History of the Pentagon Papers Case*, Berkeley, University of California Press, 1996, pp. 101, 139.

The New York Times acababa de rehusar el requerimiento gubernamental de cesar toda publicación referente a lo que hoy se conoce como los «papeles del Pentágono» y de restituir dichos documentos al Departamento de Defensa.[7] Tales papeles, extraídos en su mayoría del informe del Pentágono titulado «Historia del proceso de toma de decisiones de EEUU sobre la política en Vietnam», evaluaban la política estadounidense durante la guerra de Vietnam.[8] Su valoración era muy negativa y conducía a unas conclusiones devastadoras que dejaban en muy mal lugar al gobierno y hacían que la guerra pareciera imposible de ganar.

Estos papeles habían llegado a la redacción de *The New York Times* a través de alguien que estaba convencido de que era imposible ganar la guerra; alguien que había trabajado en el Pentágono y que colaboró en la redacción del informe; alguien que en un principio no se opuso a la guerra pero que, con el tiempo, había llegado a la conclusión de que la guerra de Vietnam estaba perdida.

Ese alguien era Daniel Ellsberg. Fue él quien cogió a escondidas una de las quince copias de los documentos depositadas en una caja fuerte de la RAND Corporation y la llevó a una copistería externa donde él y un colega, Anthony Russo, fotocopiaron los papeles durante varias semanas.[9] Ellsberg intentó sin éxito hacer públicos los documentos incluyéndolos en el Diario de Sesiones del Congreso. Al final contactó con Neil Sheehan, reportero de *The New York Times*, con la esperanza de que este diario los publicara. Ellsberg era consciente de que con ello estaba incurriendo en un delito, pero, en su opinión, el delito era la guerra en sí misma; su objetivo era hacer ver a los estadounidenses de qué clase de delito se trataba.

Durante dos meses y medio, los editores de *The New York Times* examinaron los papeles, afanándose en verificar su autenticidad y exactitud. Tras este examen pormenorizado, los editores determinaron que eran auténticos y decidieron publicar la primera de una serie de diez entregas de extractos e historias el domingo 13 de junio de 1971.[10]

El lunes 14 de junio por la tarde, un día después de la aparición de la primera entrega, el fiscal general John Mitchell envió un telegrama a *The New York Times* que exponía lo siguiente:

---

7 *Ibidem*, p. 100.

8 Véase *ibidem*, p. 2.

9 Véase *ibidem*, pp. 2, 42.

10 *Ibidem*, pp. 47, 63.

> Solicito respetuosamente que no publiquen más información de esta naturaleza y que me notifiquen que han realizado las gestiones oportunas para restituir estos documentos al Departamento de Defensa.[11]

Cuando *The New York Times* rehusó su requerimiento, el gobierno estadounidense le interpuso una demanda para vetar la publicación de historias y extractos de los documentos.[12]

Las alegaciones del gobierno eran muy simples: esos documentos contenían secretos de Estado, le habían sido sustraídos al gobierno su publicación pondría en riesgo a muchos soldados estadounidenses, avergonzaría al país delante del mundo. Esta preocupación acerca de la reputación iba más allá de la simple vanidad: dicha afrenta, afirmaba el gobierno, debilitaría la posición estadounidense en sus esfuerzos por negociar un acuerdo de paz. Debido al daño que se podría derivar de la publicación de las sucesivas entregas de esos mismos documentos, el Tribunal Supremo debía intervenir para paralizarla.

Esta argumentación no carecía de antecedentes. Con anterioridad, los tribunales ya habían paralizado la publicación de textos que amenazaban la vida de las personas, especialmente en contexto de guerra. Tal y como dictaminó el Tribunal Supremo en «Near contra Minnesota», por ejemplo, «nadie cuestionaría que un gobierno pueda impedir los obstáculos a su servicio de reclutamiento o la publicación de las fechas de partida de los transportes marinos o del número y la posición de las tropas».[13]

Con todo, la cuestión no se resolvió con facilidad. Frente a los antecedentes se erigía un mandato cada vez más claro: si algo significaba la Primera Enmienda, era que el gobierno no puede ejercer de forma generalizada el poder de censura previa.[14] La «censura previa» se da cuando el gobierno

---

11 Sanford J. Ungar, *The Papers and the Papers: An Account of the Legal and Political Battle over the Pentagon Papers*, Nueva York, Columbia University Press, 1989, p. 120; citado en Rudenstine, *The Day the Presses Stopped*, *op.cit.*, p. 92.

12 Véase Rudenstine, *The Day the Presses Stopped*, *op.cit.*, p. 105.

13 *Near vs. Minnesota,* 283 US 697, 716, 1931; cf. *United States vs. Noriega,* 917 F2d 1543, 11th Cir 1990, donde se afirma la restricción previa de la grabación de las conversaciones del acusado con su abogado sobre la base de que éstas podrían impedir la celebración de un juicio justo; revisión denegada, 498, US 976, 1990 (voto particular del juez Thurgood Marshall).

14 Véase, por ejemplo, *Organization for a Better Austin vs. Keefe*, 402 US 415, 418–19, 1971; *Bantam Books, Inc., vs. Sullivan*, 372 US 58, 70, 1963; *Near vs. Minnesota*, 283 US 697, pp. 713–714.

utiliza los tribunales para paralizar la publicación de algún material, en lugar de castigar a posteriori a quien lo publique ilegalmente. Se considera que tal poder entraña los mayores riesgos para un sistema de libertad de expresión.[15] Y el fiscal general Mitchell estaba pidiendo precisamente al Tribunal Supremo que ejerciese dicho poder.

El Supremo tuvo dificultades con la cuestión, pero la resolvió con celeridad. Los conflictos se debían al alto coste que parecía haber en el caso.[16] Sin embargo, al decidir, el Tribunal se decantó sin ambages contra el gobierno. Según la interpretación del Supremo, la Constitución otorgaba a *The New York Times* el derecho a publicar los documentos sin la amenaza de la censura previa.

El caso de los «papeles del Pentágono» constituye un clásico estadounidense en el ámbito de la libertad de expresión —un impresionante recordatorio de cuán poderosa puede llegar a ser una Constitución. Pero hasta los clásicos envejecen. Y en una conferencia que pronunció poco antes de que apareciera la primera edición de este libro, Abrams se planteaba una pregunta increíble: ¿es aún importante este caso? ¿O la tecnología ha vuelto innecesaria esta protección de la Primera Enmienda?

La pregunta de Abrams venía motivada por una idea obvia: para que el gobierno logre que se atienda su reclamación de paralizar una publicación, debe demostrar que dicha publicación ocasiona un «perjuicio irreparable»

---

15 Los argumentos tipo los resumen muy bien Kathleen M. Sullivan y Gerald Gunther: «(1) A un funcionario le es más fácil restringir la expresión "por medio de un simple trazo de bolígrafo" que mediante el más engorroso aparato del castigo subsiguiente [...]. (2) Los censores manifestarán una predisposición profesional a favor de la censura y, en consecuencia, sobrestimarán sistemáticamente los intereses estatales y subestimarán la expresión. (3) Los censores operan de modo más informal que los jueces, proporcionando así menos salvaguardas procedimentales a quienes se expresan. (4) La expresión suprimida por adelantado jamás alcanza el mercado de las ideas. (5) Cuando la expresión se suprime por adelantado, no hay pruebas empíricas con las que medir los posibles perjuicios que se le atribuyen»; *First Amendment Law*, Nueva York, Foundation Press, 1999, pp. 339–340, citando a Thomas Emerson, «The Doctrine of Prior Restraint», *Law and Contemporary Problems*, núm. 20, 1955, p. 648. Frederick Schauer ofrece una interesante contribución a esta teoría comúnmente aceptada; véase «Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect"», *Boston University Law Review*, núm. 58, 1978, pp. 685, 725–730.

16 En un intercambio de pareceres particularmente ilustrativo, el juez Stewart le preguntó al profesor Bickel acerca de un caso en el que la revelación de información «acarreara la sentencia de muerte para cien jóvenes cuyo único delito hubiera sido tener diecinueve años y ser los primeros en ser llamados a filas. ¿Qué deberíamos hacer?». Bickel replicó que «sus inclinaciones humanitarias superarían su, en cierto modo más abstracta, devoción por la Primera Enmienda en un caso de esa índole»; Peter Irons y Stephanie Guitton (eds.), *May It Please the Court: The Most Significant Oral Arguments Made Before the Supreme Court Since 1955,* Nueva York, Free Press, 1993, p. 173.

—un perjuicio tan importante e irreversible que el Tribunal Supremo debe intervenir para evitarlo.[17] Pero tal demostración depende de que no se produzca la publicación —si el *Chicago Tribune* hubiera publicado previamente los papeles del Pentágono, el Gobierno no podría haber alegado ningún interés acuciante para detener su publicación en el *New York Times*. Una vez abierta la caja de Pandora, impedir nuevas publicaciones no arregla nada.

Este argumento queda claro en un caso posterior al del *New York Times* —un caso que podría haber inventado perfectamente un profesor de derecho. A finales de la década de los setenta, la revista de tendencia izquierdista *The Progressive* encargó a Howard Morland un artículo acerca de las investigaciones sobre la bomba de hidrógeno. Antes de publicarlo, *The Progressive* presentó el manuscrito al Departamento de Energía, y el gobierno le respondió con un requerimiento judicial para bloquear su publicación. Las alegaciones gubernamentales eran apremiantes: revelar al mundo los secretos sobre la fabricación de la bomba permitiría a cualquier terrorista aniquilar una ciudad entera. El 26 de marzo de 1979 el juez del Distrito Occidental de Wisconsin, Robert Warren, admitió a trámite dichas alegaciones y dictó una orden de restricción temporal que prohibía a *The Progressive* publicar su artículo.[18]

A diferencia del de los papeles del Pentágono, este caso no llegó rápidamente al Tribunal Supremo. En lugar de ello, su instrucción se dilató, en parte porque el juez encargado del sumario comprendió el enorme riesgo que entrañaba esta publicación y la paralizó mientras lo analizaba. Sus deliberaciones se prolongaron durante dos meses y medio. Entre tanto, los editores de *The Progressive* recurrieron ante el Tribunal de Apelaciones y el Tribunal Supremo, reclamándoles que apresuraran estas reflexiones. Ninguno de ellos intervino.

---

17 En un fallo coincidente, el juez Potter Stewart escribió que la censura previa en cuestión no era válida, dado que él no podía afirmar que «la revelación de los papeles del Pentágono ocasionará un daño directo, inmediato e irreparable a nuestra nación o a sus ciudadanos»; *New York Times Company vs. United States*, 403 US 713, 730, 1971 (*per curiam*). Con frecuencia se ha considerado que este criterio reflejaba la postura del Supremo; véase Laurence H. Tribe, *American Constitutional Law*, Mineola (NY), Foundation Press, 1978, p. 731; Morton H. Halperin y Daniel N. Hoffman, *Top Secret: National Security and the Right to Know*, Washington DC, New Republic Books, 1977, p. 147; véase también *Alderman vs. Philadelphia Housing Authority*, 496 F2d 164, 170, 3º Cir, 1974, rev. denegada, 419 US 844, 1974 (la censura previa debe estar respaldada por «pruebas concluyentes» que demuestren que resulta «esencial para un interés vital del Estado»).

18 Véase *United States vs. Progressive, Inc.*, 467 FSupp 990, WDWis 1979; véase también L. A. Powe Jr., «The H-Bomb Injunction», *University of Colorado Law Review*, núm. 61, 1990, pp. 55, 56.

Hasta que Chuck Hansen, un programador informático, lanzó el concurso «Diseña Tu Propia Bomba H» y divulgó una carta de dieciocho páginas en la que detallaba cómo consideraba él que funcionaba una de estas bombas. El 16 de septiembre de 1979, el *Press-Connection* de Madison (Wisconsin) publicó la carta, y al día siguiente el gobierno retiró su demanda contra *The Progressive*, admitiendo que el caso era dudoso. El interés acuciante del gobierno se esfumó en cuanto el secreto vio la luz.[19]

Nótese lo que esta secuencia implica. Hay una necesidad de protección constitucional en el caso de los papeles del Pentágono únicamente porque se da una restricción real sobre la publicación. Dicha publicación requiere la presencia de un editor, el cual puede ser castigado por el Estado. Ahora bien, si una parte o todos los hechos se publican primero en otro sitio, entonces la necesidad de protección constitucional desaparece. Una vez que se publica el material, no hay ninguna justificación legal para suprimirlo.

Así pues, pregunta Abrams, ¿sería importante hoy el caso de los papeles del Pentágono? ¿Sigue siendo esencial la protección constitucional que representa?

Sorprendentemente, Floyd Abrams sugiere que no es así.[20] Hoy existe un modo de asegurarse de que el gobierno nunca tenga un interés acuciante en solicitar que un tribunal paralice una publicación. Si el *New York Times* quisiera publicar hoy los papeles del Pentágono, podría asegurarse de que éstos se hubieran publicado con anterioridad simplemente filtrándolos a un grupo de noticias de USENET, o a uno de los millones de *blogs* que existen. Mucho más velozmente de lo que se distribuye su propio periódico, los papeles del Pentágono se publicarían así en millones de lugares de todos los rincones del mundo. De esta forma, la necesidad de la protección constitucional se anularía, puesto que la arquitectura del sistema otorga a cualquiera el poder de publicar material de manera rápida y anónima.

Por consiguiente, sugiere Abrams, la arquitectura de la Red elimina la necesidad de la protección constitucional. Más aún, abunda Abrams, la Red protege contra la censura previa tal y como lo hizo la Constitución —asegurándose

---

19 El *Milwaukee Sentinel* y la revista *Fusion* habían publicado artículos que trataban conceptos similares; véase A. DeVolpi *et al.*, *Born Secret: The H-Bomb, The Progressive Case, and National Security*, Nueva York, Pergamon Press, 1981, pp. 102, 106; véase también Howard Morland, *The Secret That Exploded*, Nueva York, Random House, 1981, pp. 223, 225–226.

20 Véase Floyd Abrams, «First Amendment Postcards from the Edge of Cyberspace», *St. John's Journal of Legal Commentary*, núm. 11, 1996, pp. 693, 699.

de que ya no se puedan dar fuertes controles sobre la información. Así, la Red realiza lo que se pretendía con la publicación de los papeles del Pentágono —asegurarse de que la verdad no permanece oculta.

Ahora bien, esta historia presenta una segunda cara.

El 17 de julio de 1996, el vuelo 800 de la TWA cayó al mar a diez millas de la costa sur de Center Moriches (Nueva York), provocando la muerte de doscientas treinta personas. Inmediatamente después del accidente, las autoridades estadounidenses lanzaron la (por entonces) mayor investigación de una colisión aérea de la historia del Comité Nacional de Seguridad en el Transporte, gastándose 27 millones de dólares hasta determinar que el accidente se había debido a un fallo mecánico.[21]

Ésta no era, sin embargo, la opinión de Internet. Desde el principio, circularon por la Red historias referentes a «fuego amigo» —según las cuales se había visto cómo unos misiles impactaban contra el avión. Decenas de testigos oculares informaron de que vieron un fogonazo de luz dirigirse al avión justo antes de que este cayera. Hubo también alusiones a pruebas con misiles que la Marina llevaba a cabo a setenta millas del lugar de la colisión.[22] En definitiva, la Red sostenía que existía un complot del gobierno estadounidense para ocultar su implicación en uno de los peores desastres de la aviación civil de la historia de EEUU.

El gobierno negó tales acusaciones, pero cuanto más las negaba, más «pruebas» surgían en la Red en su contra.[23] Y entonces, como colofón de la historia, apareció un informe, supuestamente filtrado desde dentro del gobierno, en el que se confirmaba que existía una conspiración —ya que las pruebas apuntaban a que el vuelo 800 de la TWA había sido derribado por fuego amigo.[24]

---

21 El presidente del Comité Nacional de Seguridad en el Transporte, Jim Hall, anunció más tarde que las investigaciones confirmaban que una explosión en el depósito de gasolina causó el accidente; véase «Statement of Jim Hall, Chairman, National Transportation Safety Board», 16 de julio de 1998, disponible en www.ntsb.gov/pressrel/1998/980716.htm.

22 Véase Robert E. Kessler, «TWA Probe: Submarines off Long Island/Sources: But No Link to Crash of Jetliner», *Newsday*, 22 de marzo de 1997, A8.

23 Véase, por ejemplo, James Sanders, *The Downing of TWA Flight 800*, Nueva York, Kensington Publishing, 1997, pp. 131–137; Accuracy in Media *et al.*, «TWA 800—Missile Website Roadmap», disponible en http://www.angelfire.com/hi/TWA800; Mark K. Anderson, «Friendly Ire», disponible en http://personals.valleyadvocate.com/articles/twa3.html; Ian W. Goddard, «TWA Flight 800 and Facts Pertaining to U.S.Navy Culpability», disponible en http://users.erols.com/igoddard/twa-fact.htm.

24 Véase Sanders, *The Downing of TWA Flight 800*, *op. cit.*, pp. 29–30, 75, 70–79, 171–173.

El antiguo secretario de prensa del presidente John F. Kennedy dio credibilidad a este informe. En una conferencia pronunciada en Francia, Pierre Salinger anunció que su gobierno estaba ocultando los hechos relativos a este caso, y que él podía probarlo.

Recuerdo bien este episodio. Poco después de oír el informe de Salinger, yo estaba conversando con un colega, un destacado experto en Derecho Constitucional de una de las facultades más importantes de EEUU, y aproveché para contárselo todo. Ambos nos encontrábamos perdidos, sin saber qué pensar. Teníamos intuiciones contrapuestas acerca de la credibilidad del informe. Salinger no era ningún chiflado, pero ciertamente su historia era un disparate.

Finalmente resultó que Salinger había sido atrapado por la Red. Había sido engañado por el reverso de la idea expresada por Floyd Abrams. En un mundo donde cualquiera puede publicar, resulta muy difícil saber qué creer. Los editores son también sus redactores jefe, y éstos son quienes toman las decisiones acerca de qué publicar —decisiones que normalmente se rigen, al menos en parte, por la pregunta: ¿es esto cierto? Las afirmaciones no pueden verificarse por sí mismas. Nunca podemos establecer, a partir de una frase que informa de un hecho del mundo, si esa frase es cierta.[25] Así pues, además de con nuestra experiencia y conocimiento del mundo, hemos de contar con estructuras de reputación que construyan credibilidad. Cuando se publica algo, asociamos las afirmaciones con quien las publica. Si *The New York Times* dice que unos extraterrestres han secuestrado al Presidente de EEUU, la noticia se lee de forma distinta que si la publicase con idénticas palabras el tabloide *The National Enquirer*.

Cuando aparece una nueva tecnología, sin embargo, es probable que perdamos nuestras referencias. Esto no es nada nuevo. Se dice que la palabra inglesa *phony* («farsante») proviene del nacimiento del teléfono —el *phony* era el estafador que usaba el teléfono para timar a quienes sólo estaban familiarizados con la comunicación cara a cara. Deberíamos esperar que surja la misma incertidumbre en el ciberespacio, y que, con ella, las expectativas de credibilidad también se tambaleen al principio.

La argumentación de Abrams depende, pues, de un atributo de la Red que no podemos dar por sentado. Si existiesen estructuras de credibilidad en la Red, la importancia del caso de los papeles del Pentágono disminuiría considerablemente. Pero si la expresión en la Red adolece de falta de credibilidad, las protecciones de la Constitución recobran su importancia.

---

25 Podemos afirmar que algunas son falsas, por supuesto, como en «el gato estaba vivo y no estaba vivo».

La «credibilidad», sin embargo, no es una cualidad que emane de la ley o del código, sino de instituciones de confianza que ayudan al lector a discernir las fuentes fiables de aquéllas que no lo son. Así pues, el caso del vuelo 800 suscita una importante pregunta: ¿cómo podemos restablecer la credibilidad en este espacio de modo que no sea pasto de los chiflados?

En la primera edición de este libro, esa pregunta sólo podía contestarse hipotéticamente. Desde entonces hasta ahora, sin embargo, hemos comenzado a ver la emergencia de una respuesta. Y la palabra central de esa respuesta es: *blog*.

En el momento en que escribo, existen más de 50 millones de *weblogs* en Internet, los cuales no pueden describirse de una única forma. Todos difieren entre sí profundamente, y puede que en la mayoría de ellos no se escriban más que tonterías. Ahora bien, juzgar una dinámica mediante una fotografía instantánea es un error, y hay que reconocer que la estructura de autoridad que está construyendo esta dinámica es algo radicalmente nuevo.

En el mejor de los casos, los *blogs* son instancias de periodismo amateur —donde «amateur», una vez más, no significa de segunda fila o inferior, sino simplemente alguien que hace lo que hace por amor al arte y no por dinero. Estos periodistas escriben sobre el mundo —algunos desde una perspectiva política, otros desde el punto de vista de un interés particular—, pero todos ellos se apoyan en un entramado de otros escritores a la hora de elaborar una argumentación o un informe que añadan algo nuevo. La ética de este espacio se basa, así, en la conexión —de referencias y comentarios; y aunque esta conexión no sea «justa y equilibrada», produce un vigoroso intercambio de ideas.

Existe, además, una clasificación de *blogs*. Servicios como Technorati sondean constantemente el espacio de los *blogs*, observando quién enlaza a quién y qué *blogs* gozan de la mayor credibilidad. Y estas clasificaciones contribuyen a una economía de las ideas que construye una disciplina en torno a ellos. Los *blogueros* se granjean autoridad a partir de lo citados que sean por parte de otros, y tal autoridad atrae la atención de los lectores. Estamos ante un nuevo sistema de reputación, que no viene establecido por los redactores jefe o los directores generales de los medios de comunicación, sino por un abanico de colaboradores extraordinariamente diverso.

De resultas, estos periodistas amateur acaban produciendo un efecto. Cuando el vuelo 800 de la TWA se estrelló, aparecieron teorías de la conspiración que no fueron filtradas por ninguna estructura de credibilidad.

Hoy, en cambio, contamos con más estructuras de credibilidad. De esta manera, cuando Dan Rather sacó a la luz en el programa de la CBS *60 Minutes* una carta con la que pretendía demostrar un fraude del presidente George W. Bush, la blogosfera sólo necesitó veinticuatro horas para determinar que la prueba esgrimida por la CBS era falsa. Más increíble aún, la CBS tardó casi dos semanas en reconocer lo que los *blogs* habían averiguado.[26] El trabajo cooperativo de los *blogs* desveló la verdad y, de camino, abochornó a una compañía mediática muy poderosa. En contraste con el comportamiento de la CBS, los *blogueros* demostraron algo importante acerca de la madurez alcanzada por la red.

Dicha cooperación no viene avalada por más garantía que la que proporciona su proceso de trabajo. En este sentido, el proceso cooperativo más extraordinario en el ámbito de los contenidos lo representa la Wikipedia, una enciclopedia libre *online*, creada exclusivamente por voluntarios. Lanzada a comienzos de 2001, estos (literalmente miles de) voluntarios han generado ya más de dos millones de entradas en dicha enciclopedia. Existen versiones en nueve grandes lenguas (sin incluir la versión en klingon, el idioma vernáculo de la raza homónima de *Star Trek*), con casi la mitad de las entradas escritas en inglés.

El objetivo de la Wikipedia es la neutralidad. Los colaboradores pueden editar y reeditar una entrada hasta alcanzar una redacción neutral. A veces este esfuerzo fracasa —hay temas particularmente controvertidos que inevitablemente atraen feroces conflictos—, pero, en general, su labor alcanza un éxito increíble. Contando exclusivamente con el esfuerzo de voluntarios, y a través de millones de instancias de colaboración no coordinadas, se ha creado la enciclopedia más usada, y quizá la más útil, jamás escrita.

La Wikipedia, sin embargo, no puede garantizar sus resultados, ni que en un momento dado no haya algún error en sus entradas. Pero lo cierto es que nadie puede proporcionar tal garantía. De hecho, un estudio que recopiló al azar entradas de la Wikipedia y de la Enciclopedia Británica halló la misma cantidad de errores en una que en otra.[27]

---

26 Artículo inicial de la CBS acerca de la controversia: disponible en http://www.cbsnews.com/stories/2004/09/10/politics/main642729.shtml; retractación de la CBS: disponible en http://www.cbsnews.com/stories/2004/09/20/politics/main644539.shtml. Véase Howard Kurtz, «Rather Admits "Mistake in Judgment"», *Washington Post*, 21 de septiembre de 2004, A01: «... poniendo fin a una defensa de casi dos semanas de la conducta periodística de la cadena, la cual ha dañado gravemente su credibilidad, según los analistas mediáticos».

27 Jim Giles, «Internet Encyclopedias Go Head to Head», news@nature.com, 12 de diciembre de 2005, disponible en http://www.nature.com/news/2005/051212/full/438900a.html.

Ahora bien, la Wikipedia está expuesta a un cierto tipo de riesgo al que la Enciclopedia Británica no se enfrenta —la malicia. En mayo de 2005, un bromista deformó la entrada de la Wikipedia relativa a John Seigenthaler Sr. Dado que no había muchas personas controlando dicha entrada, pasaron cuatro meses hasta que el error fue detectado y corregido. A Seigenthaler este suceso no le hizo demasiada gracia y, comprensiblemente, se quejó de que la culpa la tenía la arquitectura de la enciclopedia libre.

La arquitectura de la Wikipedia podría ser diferente, pero la lección que podemos extraer de ella viene dada por la extraordinaria sorpresa que supone su éxito, no por sus fallos. Se da una colaboración sin precedentes entre personas de todo el mundo que se afanan por converger en torno a la verdad en un amplio repertorio de temas. En cierto sentido, a eso se dedica también la ciencia, si bien ésta emplea un tipo diferente de «revisión por pares» para inspeccionar sus resultados. Tal «revisión por pares» tampoco supone una garantía definitiva: en Corea del Sur, por ejemplo, estaban plenamente convencidos de que uno de sus científicos más prominentes, Hwang Woo-Suk, había descubierto una técnica para clonar células madre humanas. Y lo estaban porque las publicaciones científicas revisadas por pares habían informado de ello. Ahora bien, tuvieran o no razones para concederles credibilidad, las revistas se habían equivocado. Los hallazgos de Woo-Suk eran un fraude: este científico no había clonado células madre ni ninguna otra cosa que mereciera la atención mundial.

Los *blogs* no coordinan ningún proceso cooperativo de verificación del modo que lo hace la Wikipedia. En cierto sentido, los votos a favor de una postura concreta en un momento dado no cuentan nunca en los *blogs*, mientras que en la Wikipedia son constantemente escrutados. Pero incluso sin escrutarse dichos votos, los lectores de los *blogs* aprenden a confrontar la información para llegar a la verdad. Igual que ocurre con los testigos de un accidente (aunque mejor, ya que estos testigos gozan de buena reputación), el lector infiere lo que ha de ser cierto a partir de una multitud de percepciones. A Cass Sunstein le preocupa con razón que las normas de los *blogueros* no hayan evolucionado lo suficiente como para incluir la diversidad interna de citas.[28] Puede que esté en lo cierto. Pero sea cual sea la práctica lectora normal con respecto a los asuntos ordinarios, la diversidad de la blogosfera proporciona a los lectores una gama extremadamente amplia de puntos de vista a tener en cuenta cuando emerge un asunto de importancia

---

28 Véase Cass Sunstein, *Infortopia: How Many Minds Produce Knowledge*, Nueva York, Oxford University Press, 2006.

—como aquél que hizo saltar a Salinger. Si a ello unimos la maduración del sistema de reputación que constantemente atempera la influencia, esto significa que resulta más fácil equilibrar las posiciones extremas con la corrección que muchas voces pueden construir.

De esta forma, puede surgir una credibilidad que, aunque no sea perfecta, al menos se ve obstaculizada de forma diferente. La cadena NBC News debe preocuparse por su cuenta de resultados, ya que su línea editorial obedece cada vez más a ella. Los *blogs*, en cambio, no tienen cuenta de resultados, pues son —mayoritariamente— amateurs. La reputación supone una restricción para ambas formas de periodismo, y la competencia entre ellas las lleva a mejorar cada vez más. De esta manera, hoy disfrutamos de un entorno más rico para la libertad de expresión que hace cinco años —una prensa comercial atemperada por unos *blogs* cuya regulación se basa en una tecnología de la reputación que orienta tanto al lector como al escritor.

Con todo, los errores no desaparecerán. Cada cual tiene su ejemplo favorito: el mío es aquella ridícula historia según la cual Al Gore afirmó haber «inventado Internet». El bulo partió de una entrevista que Al Gore concedió a la CNN el 9 de marzo de 1999. En ella, respondió una pregunta acerca de qué le diferenciaba de Bill Bradley, su rival en las primarias del Partido Demócrata para las presidenciales del 2000, afirmando lo siguiente:

> Durante mi servicio en el Congreso de EEUU, tomé la iniciativa de crear Internet. Tomé la iniciativa de impulsar una amplia gama de acciones que han demostrado ser importantes para el crecimiento económico y la protección del medioambiente en nuestro país, además de para la mejora de nuestro sistema educativo.[29]

Como queda claro por el contexto, lo que Al Gore afirma no es que inventara la tecnología de Internet, sino que tomó «la iniciativa de impulsar una amplia gama de acciones» que han resultado importantes para el país. La historia, sin embargo, se contó de modo que parecía que Al Gore se arrogaba haber «inventado Internet». Y así la repitió el periodista de Internet Declan McCullagh dos semanas después: «El Vicepresidente mintió descaradamente

29 Véase Seth Finkelstein, «Al Gore "invented the Internet"—resources, transcript: Vice President Gore on CNN's *Late Edition*» (última actualización viernes 28 de abril de 2006), disponible en http://www.sethf.com/gore.

con el cuento chino de que él había inventado Internet». Tal atribución —sencillamente falsa— caló hondo. En un estudio de 2003 sobre el tratamiento mediático de la noticia, Chip Health y Jonathan Bendor concluyeron: «Mostramos que la versión falsa de las declaraciones de Al Gore se impuso ampliamente a la verdadera en el discurso político oficial. Se trata de un claro error en el mercado de las ideas, que documentamos al detalle».[30]

Lo único que se salva de esta historia es la facilidad con la que se documenta la falsedad —gracias a Internet. Seth Finkelstein, programador y activista contra la censura informática, ha creado una página en Internet en la que se recoge la entrevista original y las noticias posteriores sobre ella.[31] El suyo es el modelo óptimo de lo que Internet podría llegar a ser. Esta virtud, sin embargo, no llegó muy lejos fuera de la Red.

Regulaciones de la expresión: correo basura y pornografía

Por mucho que hablemos de nuestro amor a la libertad de expresión, lo cierto es que, en el fondo, a la mayoría de nosotros no nos importaría un poco de sana regulación, al menos en ciertos contextos. O, al menos, hoy habría más gente deseosa de dicha regulación que la que había en 1996. Este cambio viene motivado por dos expresivas categorías que se han convertido en la cruz de la existencia de muchas personas en la Red: el correo basura y la pornografía.

Por «correo basura» entiendo los correos electrónicos comerciales no solicitados que se envían de forma masiva. En esta definición, «no solicitados» se emplea en el sentido de que no existe relación alguna entre el remitente y el destinatario; «comerciales» en un sentido que excluye los correos políticos; «correos electrónicos» en el sentido no restringido a los mensajes electrónicos, sino abarcando cualquier medio de interacción en el ciberespacio (incluyendo los *blogs*); y «masiva» en el sentido de muchos (el lector ya sabe a qué cantidades me refiero) correos enviados de una vez.

---

30 *Ibidem*.
31 *Ibidem*.

Por «pornografía» entiendo, no la obscenidad ni la pornografía infantil, sino lo que el Tribunal Supremo de EEUU llama expresión sexual explícita que es «perjudicial para menores».[32] Ésta es la categoría de la expresión erótica legalmente permitida —al menos para los adultos, no para los niños—, ya que la obscenidad y la pornografía infantil están prohibidas para todos.

Estos dos tipos de expresión —la pornografía y el correo basura— son muy diferentes entre sí, pero se asemejan en la estructura de regulación que ambas demandan. Ninguna de ellas debería estar prohibida mediante regulación: hay personas a las que recibir correo basura les hace felices, del mismo modo que hay personas autorizadas constitucionalmente para acceder a la pornografía. Ahora bien, para ambos tipos de expresión existe una clase de individuos que desearía poder bloquear su acceso: la mayoría de nosotros con respecto al correo basura, y los padres con respecto a la pornografía. He aquí el deseo de una cierta forma de «regulación de la expresión». La cuestión es si la ley puede respaldarla, y cómo.

Yo estoy totalmente a favor de esta forma de regulación de la expresión, siempre que se diseñe adecuadamente. «Pero», puede que los opositores a la regulación respondan, «¿cómo puedes abrazar tan fácilmente la idea de la regulación? ¿Acaso has olvidado los importantes principios de la libertad de expresión?».

No obstante, si los amantes de esta forma de regulación de la expresión han estado leyendo atentamente, encontrarán una respuesta rápida a esta acusación de censura. Si reflexionamos sobre ello, queda claro que, en el sentido descrito en el

---

32 *Ginsberg vs. New York*, 390 US 629, 1968. La obscenidad no es un tipo de expresión constitucionalmente protegido y las leyes federales prohíben el transporte de materiales obscenos; véase 18 USCA 1462, 1984, enmendada por 18 USCA 1462, Supp 1999. En *Miller vs. California,* el Tribunal Supremo describió así la prueba de la obscenidad: «(a) si "la persona promedio, aplicando los principios contemporáneos de su comunidad" encontrara que la obra, tomada en su conjunto, apela al interés lascivo; (b) si la obra representa o describe, de un modo patentemente ofensivo, la conducta sexual específicamente definida en la ley estatal que sea de aplicación; y (c) si la obra, tomada en su conjunto, presenta graves carencias de valores literarios, artísticos, políticos o científicos»; *Miller vs. California,* 413 US 15, 24, 1973 (resolución 5-4), revisión denegada, 414 US 881, 1973. La pornografía, por otra parte, está amparada por la Primera Enmienda pero puede ser regulada para promover el interés estatal de proteger a los niños de materiales perjudiciales, siempre y cuando la regulación sea el medio menos restrictivo de promover el interés articulado; véase *Ginsberg vs. New York,* 390 US 629, 637-640, 1968. La pornografía infantil puede ser prohibida en tanto que material obsceno incluso si no se la considera obscena según la prueba de Miller, y ello debido al fuerte interés estatal en impedir la explotación sexual de los niños; véase *New York vs. Ferber,* 458 US 747, 764, 1982. La pornografía infantil no está constitucionalmente protegida, y la legislación federal prohíbe su transporte; véase 18 USCA 2252 (1984), enmendada por 18 USCA 2252, Supp 1999.

Capítulo 7, el correo basura y la pornografía siempre han estado regulados en el espacio real. El único interrogante con respecto al ciberespacio es si allí podrá conseguirse el mismo efecto que producen esas regulaciones en el espacio real.

Regulaciones del espacio real: correo basura y pornografía

Pensemos primero en el correo basura del espacio real. En el sentido del Capítulo 7, el correo basura está exhaustivamente regulado en este espacio. Tal regulación la podemos comprender a través de las cuatro modalidades que hemos analizado.

En primer lugar, la ley: las regulaciones contra el fraude y las declaraciones engañosas restringen las tretas que pueden emplear quienes envían correo masivo en el espacio real. Así, los concursos están severamente regulados (basta con echar un vistazo a las exenciones de responsabilidad incluidas en los sorteos de la *Publishers' Clearing House*).

En segundo lugar, las normas regulan el envío masivo de correo en el espacio real. Existe una conciencia acerca de qué es adecuado anunciar, y todo anuncio que queda fuera es casi contraproducente.

En tercer lugar, los mercados regulan el envío masivo de correo en el espacio real. El coste del correo en el espacio real es alto, lo que implica que debe proporcionar cuantiosas ganancias para que merezca la pena su envío masivo. Esto reduce radicalmente el volumen de correo masivo que se envía en este espacio.

Y finalmente, la arquitectura regula el envío masivo de correo en el espacio real. Recibimos el correo sólo una vez al día, y es fácil discernir entre el real y el de envío masivo. De la misma forma, resulta fácil deshacerse de este último sin tan siquiera abrirlo. En este sentido, los gravámenes del correo basura del espacio real no son excesivamente grandes.

La conjunción de estos factores restringe la expansión del correo basura en el espacio real: hay menos de lo que les gustaría a sus remitentes, incluso si sigue siendo más de lo que nos gustaría al resto. Así pues, estas cuatro restricciones regulan el correo basura en el espacio real.

Algo parecido puede decirse acerca de la pornografía.

En el espacio real, la pornografía está regulada exhaustivamente —insisto, no la obscenidad ni la pornografía infantil, sino lo que el Tribunal Supremo de EEUU llama expresión sexual explícita que es «perjudicial para menores». La obscenidad y la pornografía infantil también están reguladas, pero de forma diferente: ambas están prohibidas para todos en el espacio real (estadounidense); la pornografía, por su parte, sólo está prohibida para los niños.

También podemos comprender la regulación de la pornografía mediante las cuatro modalidades de regulación mencionadas, todas las cuales tienen un mismo fin: mantener la pornografía fuera del alcance de los niños, asegurando al mismo tiempo (a veces) que los adultos puedan acceder a ella.

En primer lugar, la ley se encarga de ello. En muchas jurisdicciones las leyes exigen que no se venda pornografía a los niños.[33] Al menos desde 1968, cuando el Supremo dictó sentencia en el caso «Ginsberg contra el Estado de Nueva York»[34], tal regulación ha sido sistemáticamente confirmada. Los Estados pueden solicitar a los vendedores de pornografía que sólo la vendan a adultos, y también obligarles a que comprueben los documentos de identidad de los compradores.

Pero, no sólo las leyes regulan la pornografía; también lo hacen las normas sociales. Éstas restringen de modo general la venta de pornografía —la sociedad, en su mayoría, siente cierto desprecio hacia quienes la consumen, y ello, sin duda, inhibe su venta. Las normas también respaldan la política de mantener la pornografía fuera del alcance de los niños. Y quienes comercian con ella no desean verse a sí mismos como corruptores de menores. Vender pornografía a niños está universalmente considerado como algo que los corrompe, y esto supone una restricción importante para los vendedores de pornografía, así como para cualquier otra persona.

También el mercado mantiene la pornografía fuera del alcance de los niños. La pornografía en el espacio real cuesta dinero, y los niños no suelen disponer de mucho. Y dado que los vendedores discriminan en función de quién puede pagar, contribuyen así a disuadir a los niños de comprar pornografía.

---

33 La jueza Sandra Day O'Connor elaboró una lista de más de 40 estados con esa clase de leyes en su dictamen coincidente en *Reno vs. ACLU*, 521 US 844, 887 n. 2.

34 *Ginsberg vs. New York* , 390 US 629, 1968.

No obstante, las regulaciones de la ley, del mercado y de las normas presuponen otra regulación que es la que las hace posibles: la regulación de la arquitectura del espacio real. Y es que en el espacio real es difícil ocultar que se es un niño. Se puede intentar, pero se está abocado al fracaso. Por consiguiente, dado que un niño no puede ocultar su edad y que la pornografía se vende mayoritariamente cara a cara, las arquitecturas del espacio real determinan que sea relativamente barato aplicar las leyes y normas.

Esta constelación de regulaciones del espacio real tiene el efecto de controlar, en una medida importante, la distribución de pornografía a los niños. La regulación no es perfecta —cualquier niño que realmente quiera material pornográfico lo puede conseguir— pero la regulación no tiene que ser perfecta para ser efectiva. Basta con que estas regulaciones consigan que la pornografía no esté disponible para los niños de forma general.

Regulaciones del ciberespacio: correo basura y pornografía

El correo basura y la pornografía son regulados de forma diferente en el ciberespacio. Es decir, esas mismas cuatro modalidades restringen o permiten el correo basura y la pornografía de forma diferente en el ciberespacio.

Empecemos esta vez por la pornografía. La primera diferencia radica en el mercado. En el espacio real, la pornografía cuesta dinero, mientras que en el ciberespacio no tiene por qué —o, al menos, no cuesta mucho. Si alguien quiere distribuir un millón de fotos de «la vecina de al lado» en el espacio real, no sería disparatado calcular que le costará en torno a un millón de dólares. En el ciberespacio, en cambio, la distribución es prácticamente gratuita. Con sólo disponer de acceso al ciberespacio y de un escáner, se puede escanear una foto de «la vecina de al lado» y luego distribuir la imagen digital a través de USENET a mucho más de un millón de personas por sólo el coste de una conexión a Internet.

Con costes de producción tan ínfimos, se produce una oferta de pornografía mucho mayor para el ciberespacio que para el espacio real. De hecho, en el ciberespacio surge toda una categoría de pornografía que no existe en el espacio real —pornografía amateur o producida sin fines comerciales— y que simplemente no podría sobrevivir.

Y luego está la demanda. En el ciberespacio se puede acceder a la pornografía —a menudo y en muchos sitios— de forma gratuita. Miles de sitios comerciales tienen disponible pornografía sin tener que pagar nada a cambio, como un reclamo para atraer a clientes. Y aún más pornografía se distribuye en contextos no comerciales, tales como USENET o las páginas de pornografía gratuita. Una vez más, estos precios tan bajos se traducen en una demanda mucho mayor.

Gran parte de esta oferta y demanda es para un mercado que, al menos en EEUU, está protegido por la Constitución. Así, en este país, los adultos gozan del derecho constitucional a acceder a la pornografía, lo que significa que el Estado no puede hacer nada que lo obstaculice (acaso que obstaculice sin una buena razón). Ahora bien, en EEUU existe otro mercado de la pornografía que no está constitucionalmente protegido, lo que implica que las autoridades estadounidenses tienen derecho a bloquear el acceso de los niños a la pornografía.

Como vimos en la sección anterior, para que dicha regulación funcione, sin embargo, tiene que haber un modo relativamente sencillo de saber quién es un niño. Pero, como hemos visto a lo largo de este libro, ésta es una característica arquitectónica de la que carece el ciberespacio. No es que en el ciberespacio los niños puedan ocultar fácilmente el hecho de que son niños, es que en él no hay hecho alguno que ocultar. Se accede sin una identidad y sólo se desvela de ella lo que uno desea —e incluso eso no puede ser autentificado con ninguna fiabilidad real. En consecuencia, en el ciberespacio un niño no tiene que revelar que es un niño, con lo que evita sufrir la discriminación que se aplica a los niños en el espacio real. Nadie tiene que averiguar que Juan es, en realidad, Juanito, con lo que la arquitectura no produce la información mínima necesaria para que la regulación funcione.

La consecuencia es que las regulaciones que tratan de bloquear selectivamente el acceso de los niños en el ciberespacio no funcionan, y esto por razones muy diferentes de las que hacen que dichas regulaciones no funcionen bien en el espacio real. En el espacio real, sin duda, hay vendedores que están dispuestos a violar la ley o que no están de entrada motivados a obedecer. En el ciberespacio, en cambio, incluso cuando el vendedor desea obedecer la ley, ésta no puede ser obedecida. Y es que la arquitectura del ciberespacio no proporciona los instrumentos para que la ley pueda cumplirse.

Algo similar puede decirse del correo basura: el correo basura constituye una actividad económica y la gente lo envía para ganar dinero. No obstante, los costes del espacio real coartan considerablemente dicho deseo. El precio de distribución del correo basura en el espacio real suponen que sólo

se envíen los proyectos que esperan obtener un beneficio económico importante. Como ya he dicho, incluso en ese caso, las leyes y normas añaden otra capa de restricción, si bien la restricción más importante la marca el coste.

Pero la eficacia de la comunicación en el ciberespacio conlleva que el coste de enviar correo basura sea radicalmente menor, lo que incrementa enormemente la cantidad de dicho correo que es razonable enviar. Incluso si se obtiene un 0,01 % de beneficio, si el coste del envío de correo basura es casi nulo, todavía se gana dinero.

Por consiguiente, al igual que con la pornografía, una restricción arquitectónica diferente comporta una regulación radicalmente diferente de la conducta. Tanto la pornografía como el correo basura están razonablemente regulados en el espacio real; en el ciberespacio, en cambio, esta diferencia de arquitectura implica que no lo estén ninguno de los dos.

Retornamos, pues, a la pregunta que abría esta sección: ¿hay un modo de «regular» la pornografía y el correo basura al menos en la misma medida en que se hacía en el espacio real?

Regulando la pornografía en la red

De todas las regulaciones posibles de la expresión en la Red (dejando a un lado el copyright por el momento), la que más ha urgido hasta ahora al Congreso estadounidense ha sido la de la pornografía. Tal urgencia, sin embargo, no se ha traducido todavía en resultados exitosos. El Congreso ha aprobado dos textos legislativos de envergadura, de los cuales el primero fue derogado completamente y el segundo va por el mismo camino en su lucha en los tribunales.

La primera ley fue producto del miedo. Justo en el momento en que la Red estaba calando en la conciencia popular, un aspecto particularmente sórdido eclipsó al resto: la pornografía. Esta preocupación pasó a ser generalizada en EEUU a comienzos de 1995.[35] Su fuente era el extraordinario

---

35 Véase Blake T. Bilstad, «Obscenity and Indecency in a Digital Age: The Legal and Political Implications of Cybersmut, Virtual Pornography, and the Communications Decency Act of 1996», *Santa Clara Computer and High Technology Law Journal*, núm. 13, 1997, pp. 321, 336-337.

incremento del número de usuarios normales de la Red y, por ende, el aún más extraordinario incremento de la disponibilidad de lo que muchos llaman pornografía en la Red. Un estudio extremadamente controvertido (y profundamente defectuoso) publicado en la *Georgetown University Law Review* informó de que la Red estaba inundada de pornografía.[36] La revista *Time*, por su parte, dedicó un reportaje de portada a la disponibilidad de pornografía en Internet.[37] De este modo, los senadores y congresistas se vieron bombardeados con exigencias de hacer algo para regular la «ciberlujuria».

El Congreso respondió en 1996 con la CDA (*Communications Decency Act*, Ley para la decencia en las comunicaciones), una ley extraordinariamente estúpida que se estrelló contra la Primera Enmienda. Esta ley establecía como delito grave la transmisión de material «indecente» en la Red a un menor o a un lugar donde un menor pudiera observarlo. Eso sí, la ley proporcionaba a los emisores de la Red una defensa —si tomaban de buena fe «medidas razonables, efectivas», para excluir a los niños, entonces sí podrían emitir «indecentemente».[38]

La CDA planteaba, como mínimo, tres problemas, cualquiera de los cuales debería haberla condenado a la autorrevocación.[39] El primero era el alcance de la expresión a la que se dirigía: la «indecencia» no es una categoría de expresión que el Congreso tenga el poder de regular (al menos fuera del contexto de la transmisión televisiva).[40] Como ya he descrito, el Congreso puede regular la expresión que es «perjudicial para menores», o expresión del «caso Ginsberg», pero ésta es muy diferente de la expresión denominada «indecente». Por consiguiente, el primer golpe a la CDA fue que llegaba demasiado lejos.

---

36 Marty Rimm, «Marketing Pornography on the Information Superhighway: A Survey of 917, 410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in over 2.000 Cities in Forty Countries, Provinces, and Territories», *Georgetown University Law Journal*, núm. 83, 1995, p. 1849. Godwin explica la historia completa del artículo de Rimm, describiendo los problemas y consecuencias más importantes de los enunciados «engañosos» y «falsos», así como su consiguiente invalidez en *Cyber Rights, op. cit., pp.* 206-259; véase también Jonathan Wallace y Mark Mangan, *Sex, Laws, and Cyberspace*, Nueva York, M&T Books, 1996, cap. 6.

37 Véase Philip Elmer-DeWitt, «On a Screen Near You: Cyberporn —It's Popular, Pervasive, and Surprisingly Perverse, According to the First Survey of Online Erotica—And There's No Easy Way to Stamp It Out», *Time,* 3 de julio de 1995.

38 47 USCA 223(e)(5)(A) Supp 1999.

39 La ley quedó revocada (al menos parcialmente) en 521 US 844, 1997; véase Eugene Volokh, «Freedom of Speech, Shielding Children, and Transcending Balancing», *Supreme Court Review*, 1997, p. 141.

40 Véase *Federal Communications Commission vs. Pacifica Foundation,* 438 US 726, 748-750, 1978 (pluralidad). Aunque el caso Pacifica ha sido duramente criticado (véase Steven H. Shiffrin, *The First Amendment, Democracy, and Romance*, Cambridge (Mass.), Harvard University Press, 1990, p. 80), continúa siendo influyente en el contexto televisivo, como aduce convincentemente Jonathan Weinberg; «Cable TV, Indecency, and the Court», *Columbia-VLA Journal of Law and the Arts*, núm. 21, 1997, p. 95.

El segundo fue su vaguedad. La forma de defensa permitida estaba clara: siempre que existiera una arquitectura que excluyera a los niños, se permitiría esta forma de expresión. Pero las arquitecturas que existían por entonces para excluir a los niños eran relativamente primitivas y, en algunos casos, bastante caras. No estaba claro si, para satisfacer la ley, tenían que ser sumamente eficaces o sólo razonablemente eficaces dada la evolución de la tecnología. En el primer caso, la defensa no constituía defensa alguna, ya que un bloqueo extremadamente efectivo era también extremadamente caro; por su parte, el coste de un bloqueo razonablemente efectivo no habría sido tan alto.

El tercer golpe fue la propia actuación del gobierno. En la defensa de su caso ante el Tribunal Supremo en 1997, el gobierno hizo bien poco por acotar el alcance de la expresión regulada o para aumentar el alcance de la defensa. Se aferró a la definición desesperadamente vaga y superficial que el Congreso había dado, y manifestó una pobre comprensión de cómo la tecnología podría proporcionar una defensa. Según el dictamen del Supremo, parecía que no había ningún modo de que un sistema de identificación pudiese ajustarse a la ley sin crear un gravamen excesivo para los emisores de Internet.

El Congreso respondió rápidamente con la aprobación de una segunda ley destinada a proteger a los niños de la pornografía, la COPA (*Child Online Protection Act*, Ley para la protección de los menores *online*) de 1998.[41] Esta ley se ajustó mejor a las exigencias constitucionales, fijándose como objetivo la regulación de la expresión perjudicial para menores. Permitió que los sitios web comerciales proporcionaran material pornográfico siempre y cuando verificaran la edad de sus visitantes. Con todo, en junio de 2003 el Tribunal Supremo prohibió su aplicación.[42]

Ambas leyes respondían a una preocupación legítima e importante. Los padres ciertamente tienen derecho a proteger a sus hijos de esta forma de expresión, y es perfectamente comprensible que el Congreso quiera ayudarles a garantizar esta protección.

Ahora bien, las dos leyes que aprobó el Congreso son inconstitucionales —y no, como sugieren algunos, porque no haya ningún modo en que el Congreso pueda ayudar a los padres. Más bien ambas leyes son inconstitucionales porque el modo concreto que se ha elegido para ayudar a los padres impone más gravámenes de los necesarios a la expresión legítima (es decir, a la dirigida a adultos).

---

41 *Child Online Privacy Protection Act* de 1998, Título XIV, Sección 1401.

42 *Ashcroft vs. ACLU*, 540 U.S. 1072, 2003.

En mi opinión, sin embargo, existe una ley perfectamente constitucional que el Congreso podría aprobar y que tendría un importante efecto en la protección de los niños contra la pornografía.

Para ver cómo sería dicha ley, hemos de retroceder un poco a la CDA y a la COPA para identificar cuáles serían los objetivos legítimos de esta regulación de la expresión.

El caso Ginsberg[43] estableció que existe una clase de expresión a la que los adultos tienen derecho a acceder, pero no los niños. Los Estados pueden regular dicha expresión para asegurarse de que llega al usuario adecuado y es bloqueada para el usuario inadecuado.

Conceptualmente, para que esa regulación funcione, hay que responder a dos preguntas:

– ¿Entra la expresión del emisor en lo «regulable» —es decir, es «perjudicial para menores»?

– ¿Está autorizado el receptor a consumir esa expresión —es decir, es menor de edad?

Y a partir de las respuestas a estas preguntas, la lógica de esta regulación es la siguiente:

SI
(expresión = regulable)
Y
(receptor = menor de edad)
ENTONCES
se bloquea el acceso

43 *Ginsberg vs. New York*, 390 US 629, 1968.

A partir de aquí, está claro que, entre el receptor y el emisor, es este último quien está en mejor posición para responder a la primera pregunta. El receptor no puede saber si la expresión es perjudicial para menores hasta que no se la encuentra, de modo que si el receptor es menor de edad, ya es demasiado tarde. Y entre el receptor y el emisor, está claro que aquél es quien está en mejor posición para responder a la segunda pregunta. De manera especial en Internet, al emisor le resulta extremadamente oneroso certificar la edad del receptor, mientras que a éste no le cuesta nada saber su propia edad.

La CDA y la COPA le atribuían al emisor la carga de responder a la primera pregunta, y tanto al emisor como al receptor la carga de responder a la segunda. Así, el emisor tenía que determinar si su expresión era regulable, y el emisor y el receptor tenían que cooperar para verificar la edad de este último. Si el emisor no lo hacía y el receptor resultaba ser menor de edad, entonces a aquél se le consideraba culpable de un delito grave.

La ley del espacio real asigna la carga exactamente del mismo modo. Si alguien quiere vender pornografía en Nueva York, necesita determinar si el contenido que vende es «perjudicial para menores» y si la persona a quien se lo vende es menor de edad. Pero el espacio real es fundamentalmente diferente del ciberespacio, al menos en el coste que implica responder a la segunda pregunta. En el espacio real, la respuesta es prácticamente automática (una vez más, un niño lo tiene difícil para ocultar que es un niño); y cuando no lo es, existe un sistema barato de identificación (un carné de conducir, por ejemplo). En el ciberespacio, en cambio, cualquier sistema de identificación obligatorio constituye una carga tanto para el emisor como para el receptor. Incluso con la COPA, un emisor tiene que pagar un sistema de tarjetas de crédito, y el receptor ha de confiar a un pornógrafo su tarjeta de crédito simplemente para acceder a una expresión protegida por la Constitución.

Hay otro rasgo más de la CDA y la COPA que, por más que parezca necesario, no lo es: ambas imponen la carga de su regulación a todas las personas, incluyendo a aquéllas que tienen derecho constitucional a acceder a material pornográfico. Es decir, ambas leyes exigen que todo el mundo muestre su documentación identificativa cuando la Constitución sólo permite bloquear el acceso a dicho material a los niños.

Así pues, comparemos las cargas que imponen la CDA y la COPA con un esquema regulador diferente: uno que desplace al emisor la carga de responder a la primera pregunta (si el contenido es perjudicial para menores) y al receptor la de responder a la segunda (si él mismo es menor de edad).

Una versión de este esquema es simple, obviamente ineficaz e injusta para el emisor: una exigencia de que el sitio web bloquee el acceso mediante una página que rece «El contenido de esta página es perjudicial para menores. Haz clic aquí si eres menor». Este esquema desplaza al niño la carga de la identificación de la edad, pero obviamente no daría ningún resultado en bloquearle el acceso y, además, de forma menos obvia, sería injusto para los emisores. Éstos pueden tener material que sea «perjudicial para menores», pero no todo el que ofrece tal material debería ser tachado de pornógrafo. Así pues, este bloqueo transparente estigmatizaría a algunos, y si fuera posible un sistema menos oneroso, dicho estigma convertiría en inconstitucional tal bloqueo.

Así pues, ¿qué alternativa hay a este esquema que pudiera funcionar realmente?

Voy a demostrar esta alternativa con un ejemplo concreto. Una vez lo comprendamos, la idea general también se captará más fácilmente.

Todo el mundo conoce el Macintosh de Apple. Éste, como cualquier sistema operativo moderno, permite ahora a los usuarios especificar «sesiones» para un ordenador concreto. Yo he generado una para mi hijo Willem (sólo tiene tres años pero quiero estar bien preparado). Cuando lo hice, establecí «controles paternos», es decir, especifiqué exactamente qué programas puede usar mi hijo y de qué tipo de acceso a Internet dispone. Estos «controles paternos» imposibilitan (de forma efectiva) la alteración de dichas especificaciones, ya que se necesita la clave de administrador para hacerlo. Y si dicha clave se mantiene en secreto, entonces el universo al que accede el niño a través del ordenador es el definido por el padre.

Imaginémonos que uno de los programas que yo pudiese seleccionar fuese un navegador con una función que podríamos llamar «modo de navegación infantil» (MNI). Tal navegador estaría programado para buscar una determinada marca en cualquier página web. Llamémosla la marca «perjudicial para menores» (<PPM> para abreviar). Esa marca o, en el lenguaje de Internet, esa *etiqueta*, pondría entre paréntesis cualquier contenido que el emisor considere «perjudicial para menores», y el navegador MNI ocultaría todo el contenido marcado con ella. Así, por ejemplo, una página web marcada así «Blablabla <PPM>bloquee esto<PPM> blablabla» aparecería en la pantalla de navegación infantil así: «Blablablablablabla», es decir, eliminando el contenido marcado como perjudicial para menores.

Así, si el mundo de Internet estuviese marcado con etiquetas <PPM>, y si los fabricantes de navegadores incorporasen en ellos esta función de filtración <PPM>, entonces los padres serían capaces de configurar sus ordenadores de modo que sus hijos no tuvieran acceso a ningún contenido marcado como <PPM>. El objetivo de la política de permitir el control paterno se lograría con una mínima carga sobre los emisores autorizados constitucionalmente.

Ahora bien, ¿cómo podemos conseguir que (la mayor parte del) mundo de Internet marque su contenido perjudicial para menores con etiquetas <PPM>?

He ahí la función del gobierno. A diferencia de la CDA o la COPA, la regulación exigida para hacer funcionar este sistema —hasta el punto de que funcione, y en eso se insistirá más abajo— supone simplemente que los emisores marquen su contenido. No se les exigiría que bloquearan el acceso, ni tampoco que verificasen la edad de quienes visitan su página; tan sólo se les exigiría que marcasen el contenido considerado perjudicial para menores con la etiqueta correspondiente.

Esta etiqueta, además, no equivaldría a un sambenito que clasificara una página web como pornográfica. Esta propuesta no es como las propuestas (estúpidas, en mi humilde opinión) de que creemos dominios de Internet del tipo .sex o .xxx. La gente no debería tener que trasladarse a un *barrio rojo* sólo por albergar material para adultos en su web. La etiqueta <PPM>, en cambio, quedaría oculta para el usuario normal —a menos que vaya buscándola o que quiera bloquear él por sí mismo dicho contenido.

Una vez que el gobierno promulgara una ley de este tipo, los fabricantes de navegadores tendrían un incentivo para incorporar esta tecnología de filtración (muy simple) en sus productos. Es más, dada la tecnología del navegador de código abierto Mozilla —a la que cualquiera podría añadir lo que desease—, el coste del desarrollo de este navegador modificado resultaría extremadamente bajo. Y una vez que el gobierno promulgase esta ley, y que los fabricantes construyesen un navegador que reconociera esta etiqueta, los padres dispondrían de una muy buena razón para adoptar plataformas que les permitiesen controlar a qué sitios de Internet acceden sus hijos.

Por lo tanto, en esta solución la *ley* crea un incentivo (a través de sanciones por incumplimiento) para que los sitios que contengan material «perjudicial para menores» modifiquen su *arquitectura* (añadiendo etiquetas <PPM>), lo cual crea un *mercado* para los fabricantes de navegadores (nuevos mercados) para que añadan filtros a sus productos de modo que los padres puedan proteger a sus hijos. La única carga derivada de esta

solución recae en el emisor, sin gravar en lo más mínimo al consumidor legítimo de pornografía. Para éste, no se produce ningún cambio en el modo en que experimenta la navegación por la red, puesto que la etiqueta <PPM> es invisible para aquellos consumidores que carezcan de un navegador que las busque.

Pero ¿no es inconstitucional tal carga sobre el emisor? Es difícil ver por qué sería así, dado que en el espacio real es constitucional exigir que los emisores filtren su contenido «perjudicial para menores» de cara al público infantil. Sin duda, esto supone una carga, pero la cuestión constitucional no se refiere a eso, sino a si existe un modo menos oneroso de alcanzar este importante interés estatal.

Pero ¿qué ocurre con las páginas webs extranjeras? «Los estadounidenses no pueden regular lo que ocurre en Rusia», pensará el lector. En realidad, esto es menos cierto de lo que el lector cree. Como veremos en el siguiente capítulo, el gobierno estadounidense puede hacer y hace mucho para controlar de forma efectiva lo que hacen otros países.

Con todo, puede que al lector le preocupe que los sitios extranjeros no acaten la ley estadounidense, ya que no es probable que se envíe a la Marina a clausurar un sitio web que no se atenga a dichas normas. Eso es cierto, sin duda. Ahora bien, en la medida en que a los padres les preocupe esto, existe, como ya he descrito, un mercado que permite la filtración geográfica de contenido. El mismo navegador que filtra a partir de la etiqueta <PPM> podría, en principio, suscribirse a un servicio de mapeo IP que sólo permita el acceso a páginas web estadounidenses.

Pero ¿acaso los niños no sortearán tal restricción? Por supuesto, algunos lo lograrán. Pero la medida del éxito de la legislación (al contrario de lo que ocurre con el software de seguimiento de misiles) no es del 100%. La cuestión que se plantean los legisladores es si la ley mejorará las cosas.[44] Bloquear de manera sustancial el acceso al contenido marcado con la etiqueta <PPM> constituiría una mejora significativa, lo cual basta para que la ley tenga sentido.

---

44 Hay también una doctrina en la legislación relativa a la Primera Enmienda que podría limitar la capacidad reguladora del gobierno cuando la regulación es ineficaz. Véase *Reno vs. ACLU*, 929 F. Supp 824, 848 (D. Pa. 1996), donde el tribunal explica cómo esta regulación no funcionaría en cualquier caso en las jurisdicciones extranjeras.

Pero ¿por qué no fiarse simplemente de los filtros que los padres y las bibliotecas instalan en sus ordenadores? Los filtros voluntarios no requieren una nueva legislación y, por ende, no requieren ninguna censura patrocinada por el Estado para alcanzar sus fines.

He aquí la postura que deseo analizar a fondo con el fin de refutarla, ya que contiene todos los errores que una interpretación previa al ciberderecho introduce en el debate acerca de la regulación en el ciberespacio.

Consideremos, en primer lugar, qué significa el término «censura». Lo que esta regulación haría sería proporcionar a los padres la oportunidad de realizar una importante elección, lo cual ha sido estimado como un interés estatal acuciante. Puede que los niños que no puedan acceder a este contenido porque sus padres realizaron dicha elección la tachen de «censura», pero ésta no es una aplicación muy útil del término. Si hay una razón legítima para bloquear esta forma de acceso, ésa es la regulación de la expresión, por lo que no hay justificación alguna para tacharla de nada.

En segundo lugar, hemos de considerar la preferencia por los «filtros voluntarios». Si este tipo de filtros lograra el mismo objetivo (bloquear la expresión «perjudicial para menores», y nada más que ésta), yo los apoyaría sin fisuras. Pero no lo hacen. Como la Unión Americana por las Libertades Civiles (ACLU) describió de forma muy contundente (poco después de ganar el caso que derogó la CDA, en parte con el argumento de que los filtros privados suponían un medio menos restrictivo que la regulación estatal):

> Los rescoldos de la CDA aún estaban humeantes cuando la Casa Blanca convocó una cumbre para alentar a los usuarios de Internet a autocalificar su expresión y para instar a los líderes de la industria a desarrollar e implementar las herramientas para bloquear la «expresión inadecuada». La cumbre era «voluntaria», por supuesto: la Casa Blanca defendió que con ella no estaba poniendo a nadie entre la espada y la pared. [Pero] la ACLU y otras [organizaciones] se mostraron verdaderamente alarmadas por el tenor de la cumbre de la Casa Blanca y por el firme entusiasmo hacia las soluciones tecnológicas que facilitaran el bloqueo o la invisibilidad de las expresiones controvertidas. [...] Lo que causó nuestra alarma no fue una propuesta o un anuncio en concreto, sino el fracaso de la cumbre a la hora de examinar las implicaciones para Internet de los proyectos de calificación y bloqueo a largo plazo.[45]

---

45 Ann Beeson y Chris Hansen, «Fahrenheit 451.2: Is Cyberspace Burning?», American Civil Liberties Union White Paper, 17 de marzo de 2002.

La preocupación de la ACLU es obvia: los filtros creados por el mercado no sólo van más allá de los legítimos intereses que el Estado tiene en este ámbito —el bloqueo de la expresión «perjudicial para menores»—, sino que además lo hacen de un modo completamente opaco. Se han dado multitud de historias terribles acerca de sitios que han sido incluidos en estos filtros por las razones más disparatadas (entre ellas, por criticar el propio filtro).[46] Y cuando esto ocurre, no se puede hacer demasiado. El filtro es sólo una lista de recomendaciones particularmente eficaz. No se puede demandar a la Guía Michelín sólo porque recomiende a los clientes acudir a la competencia.

Lo que defiendo aquí no es que debamos prohibir los filtros, ni tampoco que a los padres no se les deba permitir bloquear más expresiones que las consideradas «perjudiciales para menores». Lo que defiendo es que si confiamos en la acción privada por sí sola, se bloquearán más expresiones de las que bloquearía el Estado actuando con prudencia y eficacia.

Y con ello introduzco mi crítica final: como he argumentado desde el principio, deberíamos centrarnos en la libertad de expresión, y no sólo en el papel del Estado en su restricción. Así pues, entre dos «soluciones» a un problema concreto relativo a la expresión, una que involucra al Estado y suprime mínimamente la expresión, y otra que prescinde de éste pero restringe ampliamente la expresión, los principios constitucionales deberían inclinarnos a favorecer la primera. Los principios de la Primera Enmienda deberían conducir (incluso si la propia Primera Enmienda no lo hace directamente) a favorecer un sistema de regulación de la expresión que sea escueto y fiable, y en el que la acción o inacción estatal sólo conduzca a la supresión de aquella expresión que el Estado tenga un interés legítimo en suprimir. O, dicho de otro modo, el hecho de que el Estado esté involucrado en la regulación no debería necesariamente descalificar una solución adecuada que proteja nuestros derechos.

Los filtros privados que el mercado ha producido hasta el momento son caros y además se extralimitan, llegando a bloquear contenidos que van más allá de los intereses estatales de regulación de la expresión. De hecho, si reciben subvenciones es porque no existe ninguna alternativa menos restrictiva.

---

46 No todos estos filtros funcionan mediante el uso de listas negras. Dos ejemplos de programas de filtración que emplean un enfoque algorítmico en lugar de listas negras son el SafeScreen de PixAlert (disponible en www.safescreen.net) y el ImageSeeker de LTU Technologies (disponible en http://www.ltutech.com/en/), siendo este último presuntamente usado por el FBI y el Departamento de Seguridad Interior en sus investigaciones sobre pornografía infantil.

Los filtros exigidos públicamente (que son los que la etiqueta <PPM> posibilita en la práctica) están constreñidos al interés legítimo del Estado. Y si se produce una controversia acerca de dicha etiqueta —si, por ejemplo, un fiscal alega que un sitio web con información sobre el cáncer de mama debe etiquetar la información como «perjudicial para menores»—, entonces el sitio tiene al menos la oportunidad de luchar. Si tal filtro se encontrara en un software privado, no existiría oportunidad alguna de luchar contra ella por medios legales. Todo lo que los activistas de la libertad de expresión podrían hacer en ese caso es escribir artículos enérgicos, pero en gran medida invisibles, como el famoso alegato de la ACLU.

Las principales organizaciones de derechos civiles han necesitado demasiado tiempo para reconocer esta amenaza privada a los principios de la libertad de expresión. La tradición de los derechos civiles se centra directamente en la acción estatal en sí misma. Yo sería el último en afirmar que los desmanes del Estado no acarrean un enorme peligro, pero también son peligrosos para la libertad de expresión los desmanes de naturaleza privada. Un rechazo obsesivo a confrontar estos dos tipos de amenaza no contribuye en nada a los principios de la Primera Enmienda.

Pero entonces, ¿qué pasa con las tecnologías de filtración pública, como la PICS? ¿No supondría la PICS una solución al «problema de la lista secreta» que acabamos de identificar?

PICS es un acrónimo cuyas siglas corresponden a la Plataforma de Selección de Contenidos de Internet (*Platform for Internet Content*) del World Wide Web Consortium. En el capítulo dedicado a la privacidad conocimos a un pariente (a un hijo, en realidad) de la PICS: la Plataforma de Preferencias de Privacidad (*Platform for Privacy Preferences*, P3P). Al igual que la PICS, el P3P es un protocolo para clasificar y filtrar el contenido en la Red. En el contexto de la privacidad, el contenido se componía de afirmaciones acerca de las prácticas de privacidad, y el régimen estaba diseñado para ayudar a los individuos a negociar dichas prácticas.

Con respecto a la expresión en Internet, la idea es prácticamente la misma. La PICS divide el problema de los filtros en dos partes —el etiquetado (la calificación del contenido) y, a continuación, el filtro (el bloqueo del contenido a partir de esa calificación). La idea era que los diseñadores de software compitieran por escribir programas que pudiesen filtrar de acuerdo a las calificaciones, al tiempo que los proveedores de contenido y las organizaciones calificadoras compitieran por etiquetar dicho contenido. A partir de ahí, los usuarios seleccionarían su software de filtros y su sistema de calificación. Así, si el lector deseara atenerse a la

calificación de la derecha cristiana, por ejemplo, podría seleccionar su sistema de etiquetado; y si yo deseara atenerme a la calificación de la izquierda atea, podría hacer lo propio. Al seleccionar nuestra instancia de calificación, seleccionaríamos qué contenidos deseamos que filtre el software.

Este régimen requiere una serie de suposiciones. En primer lugar, los fabricantes de software tendrían que escribir el código necesario para filtrar el material. (Este paso ya se ha dado en algunos navegadores importantes). En segundo lugar, las organizaciones calificadoras tendrían que etiquetar activamente la Red. Esto, por supuesto, no sería una tarea fácil; dichas organizaciones no han asumido el reto que plantean miles de millones de páginas web. En tercer lugar, las organizaciones que etiquetaran la Red de una manera que permitiese la traducción sencilla de un sistema de calificación a otro dispondrían de una ventaja competitiva sobre el resto. Podrían, por ejemplo, vender un sistema de calificación al gobierno de Taiwán y luego desarrollar con facilidad un sistema ligeramente diferente para el «gobierno» de IBM.

Si estas tres suposiciones resultaran ciertas, podrían aplicarse a la Red innumerables calificaciones. Tal y como la imaginaron sus autores, la PICS sería neutral respecto a las calificaciones y respecto a los filtros, limitándose a proporcionar un lenguaje con el que poder calificar el contenido de la red y decidir cómo usarlo de un ordenador a otro.[47]

La neutralidad suena bien. Parece una idea que los responsables políticos deberían adoptar. La expresión de una persona no es la expresión de otra, y somos libres tanto de decir como de escuchar lo que queramos. Deberíamos establecer regímenes que protejan esa libertad, y la PICS parece ser precisamente uno de ellos.

---

47 Paul Resnick, «PICS-Interest@w3.0rg,Moving On», 20 de enero de 1999, disponible en http://lists.w3.org/Archives/Public/pics-interest/1999Jan/0000.html; Paul Resnick, «Filtering Information on the Internet», *Scientific American*, núm. 106, marzo de 1997, también disponible en http://chinese-school.netfirms.com/Internet-filtering.html; Paul Resnick, «PICS, Censorship, and Intellectual Freedom FAQ», disponible en http://www.w3.org/PICS/PICS-FAQ-980126.html; Paul Resnick y JimMiller, «PICS: Internet Access Controls Without Censorship», Communications of the ACM, núm. 39, 1996, p. 87, también disponible en http://www.w3.org/PICS/iacwcv2.htm; Jim Miller, Paul Resnick *et al*., «PICS 1.1 Rating Services and Rating Systems—and Their Machine-Readable Descriptions», 31 de octubre de 1996, disponible en el enlace http://www.w3.org/TR/REC-PICS-services; Tim Krauskopf, Paul Resnick *et al*., «PICS 1.1 Label Distribution—Label Syntax and Communication Protocols», 31 de octubre de 1996, disponible en el enlace http://www.w3.org/TR/REC-PICS-labels; Christopher Evans, Paul Resnick *et al*., «W3C Recommendation: PICS Rules 1.1, REC-PICS, Rules-971229», 29 de diciembre de 1997, disponible en http://www.w3.org/TR/REC-PICSRules.

Ahora bien, la PICS contiene más «neutralidad» de la que pudiera gustarnos. La PICS no es sólo horizontalmente neutral —permitiendo a los individuos elegir aquél que deseen entre una gama de sistemas de calificación—, sino que también es neutral en sentido vertical —permitiendo que se imponga el filtro en cualquier nivel de la cadena de distribución. La mayoría de los que respaldaron al principio el sistema imaginaron el filtro PICS alojado en el ordenador de un usuario, funcionando de acuerdo con sus deseos. Pero no hay nada en el diseño de la PICS que impida que las organizaciones que proporcionan acceso a la red filtren también el contenido. Y es que los filtros pueden darse en cualquier nivel de la cadena de distribución —el usuario, la empresa a través de la cual obtiene su acceso, el proveedor de servicios de Internet, o incluso la jurisdicción bajo la que se halla el usuario. Es decir, nada en el diseño de la PICS exige que esos filtros se anuncien a sí mismos, con lo que la filtración en esa arquitectura puede ser invisible. De hecho, en algunas de sus implementaciones la invisibilidad forma parte de su diseño.[48]

Esto debería hacer saltar las alarmas de los defensores de los principios de la Primera Enmienda —por más que el protocolo sea totalmente privado. Una consecuencia (acaso) imprevista del régimen de la PICS es que no sólo permite filtros opacos, sino que, al producir un mercado de este tipo de tecnología, engendra filtros que van mucho más allá de la expresión del «caso Ginsberg». Ésta, por supuesto, fue la queja legítima de la ACLU contra la CDA original, pero en este caso el mercado, cuyos gustos son los gustos de la comunidad, facilita los filtros. Las normas de una comunidad están integradas en el filtro, normas que son más amplias que el estrecho filtro del «caso Ginsberg». De este modo, el sistema de filtración puede expandirse tanto como lo deseen los usuarios, o hasta un nivel tan alto en la cadena de distribución como deseen las fuentes.

La alternativa que representa la suma de la etiqueta PPM y la navegación mediante MNI es mucho más restringida y permite una suerte de zonificación privada de la expresión. Sin embargo, los emisores no tendrían incentivos para bloquear a sus receptores; el incentivo de un emisor es contar con más receptores, nunca con menos. Los únicos requisitos para excluir a determinados receptores serían aquéllos que pueden ser impuestos constitucionalmente —los requisitos del «caso Ginsberg». Y puesto que sería el Estado el que los impondría, tales requisitos podrían confrontarse con la Constitución, de modo que cualquier extralimitación estatal podría ser comprobada.

---

48 Véase Jonathan Weinberg, «Rating the Net», *Hastings Communications and Entertainment Law Journal*, núm. 19, 1997, pp. 453, 478, n. 108.

La diferencia entre estas dos soluciones radica, pues, en la posibilidad de generalizar los regímenes. El régimen de filtros establecería una arquitectura que podría usarse para filtrar cualquier tipo de expresión, con lo que cabría esperar que las ansias de filtración sobrepasaran el mínimo establecido en la Constitución; el régimen de zonificación establecería una arquitectura de bloqueo que carecería de este propósito más general.

¿Qué régimen deberíamos preferir?

Fijémonos en los principios implícitos en cada régimen. Ambos representan soluciones generales a problemas particulares. El régimen de filtros no se limita a la expresión del «caso Ginsberg», sino que puede ser utilizado para calificar y filtrar cualquier contenido de Internet. Y el régimen de zonificación, en principio, no se limita a zonificar únicamente con respecto a la expresión del «caso Ginsberg». La solución zonificadora basada en la identificación infantil mediante etiquetas <PPM> podría usarse para promover otros regímenes de protección infantil. Por consiguiente, ambos regímenes poseen aplicaciones que van mucho más allá de lo concerniente a la pornografía en la red.

Al menos en principio. Deberíamos preguntarnos, no obstante, qué incentivos hay para extender estas soluciones más allá del problema inicial. Y también acerca de la resistencia que existe a tal extensión.

Aquí empezamos a vislumbrar una importante diferencia entre los dos regímenes. Cuando se nos bloquea el acceso debido al certificado que llevamos, queremos saber el porqué; cuando se nos dice que no podemos entrar en un determinado sitio web, al menos la persona excluida verifica la justificación de la exclusión. A veces dicha exclusión está justificada, pero cuando no es así, podemos desafiarla. Así pues, la zonificación incorpora en sí misma un sistema para su propia limitación, por el cual un sitio web no puede bloquear el acceso a alguien sin que éste lo sepa.[49]

El régimen de filtros es diferente. Si no podemos ver el contenido, no podemos saber qué está siendo bloqueado. El contenido podría filtrarse mediante un filtro PICS situado en algún nivel de la cadena de distribución por encima del usuario, y éste no se percataría necesariamente de lo que está ocurriendo. Nada en el diseño de la PICS exige la veracidad del bloqueo del

---

49 Esta afirmación, por supuesto, es demasiado categórica. El sitio web podría bloquear el acceso engañosamente, haciendo que parezca que el usuario accede a él, sin que en realidad se le permita acceder a lo que él cree que está accediendo.

modo en que lo hace la solución zonificadora. En consecuencia, los filtros desde arriba devienen más fáciles, menos transparentes y menos costosos con la PICS.

Este efecto queda aún más claro si consideramos por separado los componentes del proceso de filtros. Recordemos que los dos elementos de las soluciones de filtros eran el etiquetado del contenido y el bloqueo posterior basado en dicho etiquetado. Podríamos argumentar que el primero es el más peligroso, ya que si se etiqueta el contenido, entonces es posible limitar quién accede a qué sin necesidad de bloquearle el acceso. Esto podría provocar mayor inquietud que el propio bloqueo, dado que éste al menos pone al usuario sobre aviso.

Estas posibilidades deberían preocuparnos únicamente si tenemos razones para cuestionar el valor de los filtros de forma general, y de los filtros desde arriba en particular. Yo creo que sí las tenemos, pero he de confesar que mi preocupación radica en otra ambigüedad latente de nuestro pasado constitucional.

Los filtros poseen un valor innegable. Todos nosotros desechamos mucho más de lo que procesamos, y en general es mejor si podemos seleccionar nuestros filtros en lugar de que otros los seleccionen por nosotros. Si prefiero *The New York Times* a *The Wall Street Journal*, estoy seleccionando un filtro de acuerdo con mi entendimiento de los valores de ambos periódicos. Obviamente, en cualquier caso concreto, esto no plantea ningún problema.

No obstante, enfrentarnos a lo que nuestros filtros desechan también posee un valor. Individualmente podemos querer evitar cuestiones relacionadas con la pobreza o la desigualdad, y así podríamos preferir excluir esos hechos de nuestro universo informativo. Desde el punto de vista de la sociedad, sin embargo, sería terrible que los ciudadanos pudiesen simplemente excluir los problemas de los demás, ya que son esos mismos ciudadanos quienes han de elegir a líderes que los resuelvan.[50]

---

50 Véase Richard Thompson Ford, «The Boundaries of Race: Political Geography in Legal Analysis», *Harvard Law Review*, núm. 107, 1994, pp. 1841-1844, donde afirma que las fronteras jurisdiccionales perpetúan la segregación racial y la desigualdad; Gerald E. Frug, «Universities and Cities», *Connecticut Law Review*, núm. 30, 1998, pp. 1199, 1200, donde explica cómo las universidades erigen fronteras para separarse de la pobreza circundante y sostiene que las universidades deberían criticar dichas fronteras; Lani Guinier, «More Democracy», *University of Chicago Legal Forum*, 1995, pp. 1-3, donde aboga por una democracia participativa interracial que exija una preocupación por, y una familiaridad con, las opiniones ajenas.

En el espacio real, no tenemos que preocuparnos demasiado de este problema porque la filtración suele ser imperfecta. Por mucho que yo desee ignorar el problema de la vivienda, no puedo ir al banco sin tropezarme por la calle con gente «sin techo»; por mucho que desee ignorar la desigualdad, no puedo conducir al aeropuerto sin atravesar barrios que me recuerdan cuánta desigualdad hay en EEUU. Toda clase de asuntos en los que preferiría no pensar se abren paso hasta mí, exigiendo mi atención en el espacio real, independientemente de mis opciones de filtración.

Por supuesto, esto no es cierto para todo el mundo. Las personas muy ricas pueden sustraerse a aquello que no quieren ver. Pensemos en el mayordomo de una mansión inglesa decimonónica, que atiende la puerta y despacha a quienes considera que no deberían importunar a su amo. Esa clase de gente sí vivía una vida perfectamente filtrada. Y algunos la siguen viviendo en la actualidad.

En cualquier caso, para la mayoría de nosotros no es así. Debemos enfrentarnos a los problemas de los demás y reflexionar sobre los asuntos que afectan a nuestra sociedad. Tal exposición nos convierte en mejores ciudadanos.[51] Podemos deliberar y votar mejor sobre los asuntos que afectan a los demás si tenemos cierto conocimiento acerca de los problemas a los que hacen frente.

¿Qué sucede entonces si desaparecen las imperfecciones de los filtros? ¿Qué sucede si cada uno puede, de hecho, tener un mayordomo? ¿Sería ese mundo coherente con los principios de la Primera Enmienda?

Hay quien cree que no. Cass Sunstein, por ejemplo, ha sostenido de forma bastante enérgica que los fundadores de EEUU adoptaron lo que él denomina una concepción «madisoniana» de la Primera Enmienda.[52] Esta concepción rechaza la noción de que la combinación de discursos deba elegirse únicamente en función de opciones individuales,[53] insistiendo, según

---

51 Véase *Regents of the University of California vs. Bakke,* 438 US 265, 312, 1978 (el juez Lewis F. Powell, citando el caso *Keyishian vs. Board of Regents,* 385 US 589, 603, 1967: «El futuro de la Nación depende de líderes formados a través de una amplia exposición al sólido intercambio de ideas que descubre la verdad "a partir de una multitud de lenguas, [en lugar de] a través de cualquier forma de selección autoritaria"»).

52 Véase Sunstein, *Democracy and the Problem of Free Speech*, Nueva York, Free Press, 1995, pp. xvi–xx; Owen Fiss, *The Irony of Free Speech*, Cambridge (Mass.), Harvard University Press, 1996, pp. 3, 37–38; el brillante análisis de Andrew Shapiro acerca del planteamiento de Sunstein se ajusta mejor a las realidades de la Red; véase *The Control Revolution*, *op. cit.*, pp. 107–112.

53 Sunstein, *Democracy and the Problem of Free Speech*, *op. cit.*, pp. xvi–xx.

defiende Sunstein, en asegurar nuestra exposición al repertorio de asuntos que hemos de comprender para actuar como ciudadanos. En consecuencia esta concepción rechazaría cualquier arquitectura que hiciese prevalecer las opciones del consumidor. Estas elecciones no constituyen una circunstancia negativa en el esquema madisoniano, pero tampoco suponen el cierre de la cuestión. Ithiel de Sola Pool sostiene una idea muy similar:

> ¿Qué implicará la progresiva fragmentación de las audiencias en grupos más pequeños con intereses especiales? ¿Qué implicará que la agenda de manías y preocupaciones nacionales deje de ser establecida efectivamente por unos pocos medios masivos a los que todo el mundo esté expuesto? Esta tendencia plantea a la sociedad los problemas inversos de los que suscitaba el conformismo masivo. La cohesión y el funcionamiento eficaz de una sociedad democrática depende de algún tipo de ágora pública donde todos participen y aborden una agenda común de problemas, independientemente de cuánto pueda discutirse acerca de sus soluciones.[54]

Del otro lado encontramos a eruditos como Geoffrey Stone, que insiste con la misma vehemencia en que tal ideal paternalista no aparece por ninguna parte en la concepción de la libertad de expresión que abrazaron los redactores de la Constitución.[55] La Primera Enmienda, sostiene Stone, se ocupa únicamente de prohibir el control estatal de las opciones privadas. Dado que permitir dichas opciones no supone ningún problema bajo este régimen, tampoco lo suponen los filtros perfectos.

Este conflicto entre brillantes juristas de la Universidad de Chicago revela otra ambigüedad latente, y al igual que ocurre con las demás, no creo que podamos ir muy lejos mediante la apelación a Madison. Para usar los argumentos de Sunstein contra él mismo, la Primera Enmienda era un acuerdo teorizado de forma incompleta, y es mejor limitarse a confesar que no abarcó la cuestión del filtro perfecto. Los redactores de la Constitución no pudieron imaginar un mundo filtrado mediante la PICS, por lo que ciertamente no se pusieron de acuerdo en el alcance de la Primera Enmienda en tal mundo. Si hemos de apoyar un régimen por encima de otro, debemos hacerlo manifestando los principios que deseamos adoptar, más que alegando que éstos ya han sido adoptados.

---

54 Ithiel de Sola Pool, *Technologies Without Boundaries: On Telecommunications in a Global Age*, Eli M. Noam (ed.), Cambridge (Mass.), Harvard University Press, 1990, p. 15.

55 Véase Geoffrey Stone, «Imagining a Free Press», *Michigan Law Review*, núm. 90, 1992, pp. 1246, 1264.

Así pues, ¿qué principios deberíamos elegir? En mi opinión, no deberíamos optar por los filtros perfectos.[56] No deberíamos diseñar el sistema de censura más eficaz —o, por lo menos, no deberíamos hacerlo de un modo que permita la filtración invisible desde arriba. Tampoco deberíamos optar por filtros perfectos en tanto la tendencia universal sea la de filtrar en exceso la expresión. Si hay una expresión que el Estado tiene interés en controlar, entonces que lo haga de forma obvia para los usuarios. Sólo cuando la regulación es transparente es posible una respuesta política.

Por consiguiente, voto por el régimen que modifique en menor medida los principios públicos importantes. Un régimen de zonificación que permita a los niños identificarse a sí mismos supone un cambio menor que un sistema de filtros que exige, de hecho, que toda la expresión esté etiquetada. Y no sólo es un cambio menor, sino que también es menos susceptible a otras regulaciones —exige la mínima transformación de la arquitectura existente de la Red y no es fácilmente generalizable a una regulación mucho más importante.

---

56 Dan Hunter sostiene que ésta no es nuestra opción de todos modos. Véase Dan Hunter, «Philippic.com», *California Law Review*, núm. 90, 2002, p. 611. Greg Laughlin está convencido de que tal preocupación es exagerada. Véase Gregory K. Laughlin, «Sex, Lies, and Library Cards: The First Amendment Implications of the Use of Software Filters to Control Access to Internet Pornography in Public Libraries», *Drake Law Review*, núm. 51, 2003, pp. 213, 267–268, n. 287. Para una revisión del último esfuerzo del Congreso para facilitar la filtración, véase Susan P. Crawford, Symposium «Law and the Information Society, Panel V: Responsibility and Liability on the Internet, Shortness of Vision: Regulatory Ambition in the Digital Age», *Fordham Law Review*, núm. 74, 2005, pp. 1, 6: «La siguiente orden referente a membranas del flujo de información que se tramitó en el Congreso —una vez más impulsada por la fijación de los legisladores en el contenido indecente (pero legal) en la red— fue la Ley de Protección Infantil en Internet [Children's Internet Protection Act, CIPA], que exigió a las bibliotecas la instalación de programas de filtración en todos sus ordenadores con conexión a Internet para conservar su financiación federal. El objetivo de esta legislación del 2000 era condicionar la provisión de dichos fondos a que las bibliotecas usaran filtros que bloquearan el acceso a representaciones visuales que son perjudiciales para menores (cuando son menores quienes acceden a ellas). El 23 de junio de 2003, tras otros tres años de litigio, el Tribunal Supremo ratificó la CIPA, con dos jueces «vacilantes» (Anthony Kennedy y Stephen Breyer) que sugirieron que los adultos pudiesen solicitar a los bibliotecarios que desbloquearan los sitios legales (legales para un público adulto, por más que sean perjudiciales para los menores). Aunque la relación con la CDA estaba clara —se trataba de otro intento del Congreso de eliminar el material sexual de Internet empleando tecnologías que inevitablemente impedirían pasar expresiones protegidas— el vínculo con los fondos federales hizo que en este caso los jueces pudieran decidir de forma diferente. De hecho, el elemento de la financiación federal puede haber constituido la diferencia crucial entre la CDA y la CIPA. Un comentarista europeo observó el dictamen de la CIPA como una "modificación importante" por parte de un sistema legal estadounidense que había sido "anteriormente crítico con los intentos estatales de regular el acceso a Internet"».

Yo optaría por un régimen de zonificación incluso si ello requiriese una ley y la solución de filtración sólo exigiera una opción privada. Si el Estado presiona para transformar la combinación de ley y arquitectura, no me importa si en un contexto se hace mediante leyes y en otro mediante normas. Desde mi perspectiva, lo que importa es el resultado, no los medios —esto es, ¿protege el régimen producido por estos cambios los principios de la libertad de expresión?

Otros están obsesionados con esta distinción entre la ley y la acción privada. Ellos contemplan la regulación estatal como universalmente sospechosa, y la regulación por parte de agentes privados como fuera del alcance de la revisión constitucional. Y a su favor juega el hecho de que la mayoría del Derecho Constitucional está de su parte.

Sin embargo, como he indicado previamente y voy a defender más abajo, no creo que debamos dejarnos atrapar entre las líneas que trazan los abogados. Más bien deberíamos centrarnos en los principios que deseamos que el ciberespacio proteja. Ya se encargarán después los abogados de disponer cómo hacerlo.

Llegados a este punto, el fastidioso escéptico que sigue reparando en mis «incoherencias» querrá volver a darme la lata sobre esta idea. En el capítulo anterior, me decanté por una arquitectura de la privacidad que es, en esencia, la de la PICS. En efecto, el P3P, como la PICS, permitiría la negociación de contenidos entre ordenadores. El contenido del P3P consiste en reglas sobre prácticas de privacidad, y el de la PICS, en reglas sobre contenido. Pero, se pregunta el escéptico, ¿cómo puedo oponerme a una arquitectura y, al mismo tiempo, defender la otra?

La respuesta es la misma que di previamente: los principios de la expresión son diferentes de los principios de la privacidad; y el control que queremos establecer sobre aquélla es menor que el que queremos establecer sobre ésta. Por las mismas razones que inhabilitamos cierto tipo de control sobre la propiedad intelectual, deberíamos inhabilitar cierto tipo de control sobre la expresión. En el contexto de la libertad de expresión, una pizca más de desbarajuste no constituye un coste sino un valor.

Ahora bien, ¿son diferentes estos principios sólo porque yo lo diga? No. Sólo son diferentes si *nosotros* decimos que lo son. En el espacio real los tratamos como si lo fueran. Mi argumento fundamental es que hemos de elegir cómo queremos tratarlos en el ciberespacio.

Regulando el correo basura

El correo basura es quizá el problema más teorizado de la red, con decenas de libros que tratan sobre el mejor modo de abordarlo. Muchos de ellos están repletos de ingeniosas ideas técnicas para cazar el correo basura, desde avanzadas técnicas de filtración bayesiana hasta rediseños masivos del sistema de correo electrónico.

Pero lo que me resulta más asombroso como abogado (y deprimente como autor de *El código*) es que prácticamente todas estas obras ignoran una importante herramienta con la que podría abordarse el problema del correo basura: la ley. No se trata de que sopesen el valor de la ley con respecto, por ejemplo, a los filtros bayesianos o a lo último en técnicas heurísticas, y concluyan que aquélla es menos valiosa que estas otras técnicas. Es que presumen que el valor de la ley es nulo —como si el correo basura fuera una especie de gripe aviar que llevara su propia vida con total independencia de lo que los humanos puedan querer o pensar.

He aquí una omisión extraordinaria dentro de lo que es, en efecto, una estrategia reguladora. Tal y como he defendido a lo largo de este libro, la clave para una buena política en el ciberespacio es una adecuada combinación de modalidades de regulación, no una única bala de plata. La idea de que el código por sí solo puede resolver el problema del correo basura es una tontería —el código siempre puede sortearse mediante otro código y, a menos que se les incentive en otro sentido, los infractores acabarán sorteándolo. La ley constituye una herramienta para modificar los incentivos, y también debería recurrirse a ella en este ámbito.

La mayoría cree que la ley no puede desempeñar ningún papel aquí porque piensa que a los remitentes de correo basura se les dará mejor evadir la ley que evadir los filtros de correo. Pero esta forma de pensar ignora un hecho importante acerca del correo basura. El «correo basura» no es ningún virus; o, al menos, cuando hablo de «correo basura» no me refiero a ningún virus. A lo que aludo en esta parte es a la comunicación que trata de inducir una transacción comercial. Muchas de estas transacciones son ridículas —fármacos para detener el envejecimiento o pastillas de adelgazamiento instantáneo—, otras son bastante legítimas —rebajas especiales de excedentes de almacén o invitaciones para solicitar tarjetas de crédito. Pero al final todas ellas buscan sacar algo de nosotros: dinero. Y, de manera crucial, si pretenden sacar dinero de nosotros, debe haber alguien a quien le estemos dando nuestro dinero. Ese alguien debería ser, pues, el objetivo de la regulación.

Entonces, ¿qué regulación debería aplicarse?

El objetivo aquí, como con la pornografía, debería ser regular con el fin de asegurar lo que podríamos denominar «comunicación consensual». Es decir, el único propósito de la regulación debería ser bloquear la comunicación no consensuada y posibilitar la comunicación consensuada. No creo que tal propósito sea válido en todos los contextos de la expresión, pero en éste —correos electrónicos privados, o *blogs*, con un ancho de banda limitado, y receptores que han de correr con los costes de la expresión— resulta completamente adecuado regular para que los individuos puedan bloquear los mensajes comerciales que no deseen recibir.

Y ¿cómo podría lograrse eso?

Hoy la única modalidad de regulación que tiene un efecto significativo sobre el suministro de correo basura es el código. Los tecnólogos han demostrado un talento extraordinario en la concepción de técnicas para bloquear el correo basura. Estas técnicas son de dos tipos —una puesta en marcha por el contenido del mensaje, y otra puesta en marcha por el comportamiento del remitente.

La técnica que se centra en el contenido consiste en una selección de tecnologías de filtración diseñadas para descifrar el contenido del mensaje. Como describe Jonathan Zdziarski, estas técnicas han mejorado de forma prodigiosa. Mientras que las primeras técnicas de filtración heurística tenían tasas de error en torno al 10 %, las actuales técnicas bayesianas prometen una precisión que alcanza entre un 99´5 % y un 99´95 %.[57]

Pero el problema más importante de estas técnicas es la *carrera armamentística* que producen.[58] Los remitentes de correo basura tienen acceso a los mismos filtros que usan los administradores de redes para bloquearlo —al menos si los filtros son heurísticos—,[59] por lo que pueden jugar con el contenido del mensaje hasta derrotar al filtro. Esto exige entonces que los autores de

---

57 Compárese Jonathan Zdziarski, *Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification*, San Francisco, No Starch Press, 2005, p. 31 y DSPAM, disponible en http://dspam.nuclearelephant.com.

58 Zdziarski, *ibidem*, p. 25.

59 *Ibidem*, p. 31. Pero un argumento análogo puede plantearse también con respecto a la filtración bayesiana, dado que muchas de las herramientas son ellas mismas software de código abierto o libre. DSPAM, por ejemplo, utiliza la licencia GPL.

los filtros los modifiquen, lo cual algunos hacen bien y otros no. La consecuencia es que estos filtros a menudo llegan demasiado lejos, o bien se quedan cortos —bloqueando mucho más de lo que deberían o no bloqueando lo suficiente.

La segunda técnica de codificación para bloquear el correo basura se centra en las prácticas de correo electrónico del remitente —no de la persona que envía el correo electrónico, sino del «servidor» que lo reenvía al destinatario. Un gran número de vigilantes de redes —término con el que aludo a personas que actúan por el bien del mundo sin regulación legal— ha establecido listas de servidores de correo buenos y malos. Estas listas negras se compilan examinando las reglas aparentes que el servidor usa para decidir si enviar o no el correo electrónico. Aquellos servidores que no obedecen las reglas de los vigilantes acaban engrosando sus listas negras, y la gente suscrita a ellas pasa a bloquear todos los correos procedentes de esos servidores.

Este sistema sería fantástico si existiera acuerdo sobre la mejor forma de evitar los «abusos» de los servidores; pero no hay ningún acuerdo de este tipo. En su lugar existen diferencias de buena fe entre gente buena acerca de la mejor forma de controlar el correo basura.[60] Estas diferencias, sin embargo, quedan anuladas por la fuerza del boicot, que, de hecho, resulta especialmente poderoso en una red. Si cinco de cada cien destinatarios de un correo electrónico no pueden recibirlo debido a las reglas que su administrador de red adopta para su servidor de correo electrónico, podemos estar seguros de que las reglas del servidor —por más sensatas que sean— serán cambiadas. Y a menudo no hay apelación posible contra la decisión de incluir un servidor en una lista negra. Como en el caso de las tecnologías de filtros privados respecto a la pornografía, es probable que no exista remedio legal para una inclusión injusta en una lista negra.

Ahora bien, si una de estas técnicas, o las dos, realmente estuviera funcionando para detener el correo electrónico, yo las aceptaría. Me alarma particularmente el bloqueo de listas negras sin atenerse a ningún procedimiento y, personalmente, he sufrido vergüenza y costes importantes cuando mensajes que no eran correo basura fueron tratados como tal. Con todo, estos costes podrían ser aceptables si el sistema en general funcionara.

---

60 Estoy siendo benévolo. Zdziarski se muestra mucho más crítico con los «vigilantes que no observan ninguna forma de procedimiento adecuado antes de establecer listas negras de redes», *ibidem*, p. 28.

Pero no lo hace. El volumen de correo basura continúa creciendo. La consultora The Radicati Group «predice que para 2007, el 70 % de todos los correos electrónicos serán *spam*».[61] Y por más que existan pruebas de que el ritmo de crecimiento del correo basura está ralentizándose, no las hay de que la contaminación de dicho correo esté amainando.[62] La única respuesta legislativa federal, la Ley CAN-SPAM no está produciendo ningún efecto significativo, por más que priorice muchas soluciones estatales innovadoras.[63]

Pero estas técnicas no sólo no bloquean el correo basura, sino que además están bloqueando el correo masivo legítimo que —al menos desde mi perspectiva—[64] no ha de considerarse como tal. El ejemplo más importante lo constituye el correo político. Una virtud sensacional del correo electrónico era que reduciría los costes de la comunicación social y política, lo que a su vez ampliaría las oportunidades de expresión política. Pero las tecnologías de bloqueo de correo basura han surgido ahora como un gravamen sobre estas importantes formas de expresión social, eliminando en la práctica una significativa promesa que Internet ofrecía originalmente.

---

61 Véase Arik Hesseldahl, *U.S. Congress Makes No Progress on Spam*, 26 de diciembre de 2003, disponible en http://www.forbes.com/2003/11/26/cx_ah_1126tentech.html. Véase también Todd Bishop, «Software Notebook: Is Gates' prediction on spam a bust?», *Seattle Post-Intelligencer*, 23 de enero de 2006. Las estimaciones de éxito difieren aquí drásticamente. Microsoft estima que bloquea el 95 % del correo basura.

62 Jonathan Zdziarski, *op. cit.*, p. 23.

63 Véase CAN-SPAM Act of 2003, Public Law, 108-187, 2003. Para una revisión de la legislación europea, véase D. I. Cojocarasu, *Anti-spam Legislation Between Privacy and Commercial Interest: An Overview of the European Union Legislation Regarding the E-mail Spam*, Oslo, University of Oslo, 2006.

Desde mi punto de vista, definimos correo basura como «correo electrónico comercial no solicitado enviado de forma masiva». Cada uno de los elementos de la definición es necesario. «No solicitado» implica que no media un acuerdo para recibir este correo. Si tal acuerdo existe, los requisitos serían eliminados. «De forma masiva» significa que no se pretendería regular los envíos a amigos o dentro de grupos pequeños. Cf. Sonia Arrison, «Canning Spam: An Economic Solution to Unwanted Email», *Pacific Research Institute*, febrero de 2004, núm. 9. «Comercial» denota que no se regularía el correo electrónico social o político. Y «correo electrónico», acaso abarcando más que el estricto correo electrónico —quizá incluyendo, por ejemplo, el correo basura en *blogs*.

64 En mi opinión, debería permitirse que el Congreso discriminara a favor de la expresión política y pudiera, pues, eximirla de cualquier regulación relativa al «correo basura». Y ello no sólo por el valor especial de esta expresión, sino también, y aún más importante, porque el abuso de la expresión política se regula de modo más natural. Si trato de ganarme el voto del lector, no es probable que lo incordie con correo basura; pero si lo que trato es de venderle Viagra, no me importará demasiado si le incordio o no.

Así pues, tanto por haber fracasado como por estar dañando verdaderamente al menos un valor importante al que la red servía originalmente, deberíamos considerar alternativas a esta regulación exclusivamente mediante código. Y, una vez más, la pregunta es ¿qué combinación de modalidades alcanzaría mejor la legítima meta reguladora?

Comencemos con el problema: ¿por qué el correo basura es tan difícil de administrar? Simplemente porque llega sin etiquetar, de modo que no hay forma de saber si es correo basura sin abrirlo.

Esto no es algo accidental. Quienes lo envían son conscientes de que si supiéramos que se trata de correo basura, no lo abriríamos, por lo que hacen todo lo posible para hacernos creer que no lo es.

Imaginémonos por un instante que pudiéramos solucionar el problema. Imaginémonos una ley que requiriera el etiquetado del correo basura, y que esa ley funcionara. Ya sé que es extremadamente difícil imaginar algo así, pero tenga paciencia conmigo el lector. ¿Qué sucedería si todos los correos basura llegaran con una etiqueta especificada en su apartado «Asunto» —algo del tipo [PUB]?[65]

Bueno, lo que sucedería inicialmente lo sabemos. Todos nosotros (o la mayoría) solicitaríamos que nuestro cliente o nuestro servicio de correo electrónico bloquease todos los mensajes con la etiqueta [PUB] en el «Asunto». Estaríamos ante un momento glorioso en la historia del correo electrónico, un retorno a los días previos al correo basura.

Ahora bien, el resultado último de una regulación no siempre coincide con el inicial. Y con este tipo de regulación, está bastante claro que el resultado inicial sería provisional. Así, si los envíos no solicitados a buzones de correo electrónico tienen valor, este bloqueo inicial no sería sino un incentivo para encontrar vías diferentes hasta dichos buzones. Y podemos imaginarnos infinidad de esas vías:

---

65 Ésta era la ley existente en muchos Estados antes de que la Ley CAN-SPAM, de ámbito federal, impusiera su prevalencia sobre ella. Pero como dichas leyes carecían de las soluciones de aplicación que propongo aquí, no son directamente relevantes en relación al argumento que estoy exponiendo. Véase «Subject Line Labeling as a Weapon Against Spam», A CAN-SPAM Act Report of Congress, FTC, junio de 2005.

Esta solución no es más que un ejemplo de una forma general que busca transferir al remitente la carga de revelar información. Para una propuesta mucho más sofisticada, véase Theodore Loder, Marshall Van Alstyne y Rick Wash, «An Economic Response to Unsolicited Communication», *Advances in Economic Analysis and Policy*, vol. 6, núm. 1, art. 2, 2006, disponible en http://www.bepress.com/bejeap/advances/vol6/iss1/art2.

– Los remitentes podrían conseguir que los destinatarios activaran la recepción de dichos correos electrónicos. Este consentimiento los transformaría en mensajes solicitados, dejando así de ser correo basura.

– Los remitentes podrían añadir otras etiquetas en el «Asunto». Por ejemplo, si el correo basura aludiera a viajes, las etiquetas podrían ser [PUB][Viaje]. En ese caso, los receptores podrían modificar su filtro para bloquear todos los mensajes con la etiqueta [PUB] excepto los de viajes.

– Los remitentes podrían empezar a pagar a los receptores por recibir correos electrónicos. Como algunos han propuesto, el correo electrónico podría llegar con un adjunto valorado en un céntimo, o algo más. Los receptores podrían optar por bloquear todos los mensajes con la etiqueta [PUB] excepto los que les reporten algo de dinero.

La clave de estos resultados modificados es que el receptor ahora recibe los correos comerciales de forma optativa, y no engañosa. Esta evolución desde la regulación inicial fomenta, pues, que haya más comunicación, pero sólo si es consensual. Aquélla que no lo sea —asumiendo nuevamente que la regulación fuera obedecida— quedaría (en gran medida) eliminada.

Así pues, acabo de resolver en una página el problema del correo basura —asumiendo, eso sí, que se obedece la regla del etiquetado. Ahora bien, se trata, por supuesto, de una asunción imposible. ¿Qué remitente de correo basura acataría esta regulación, sabiendo que su efecto inicial sería una radical reducción de su mercado?

Para responder a esta pregunta, comencemos por retomar aquel hecho obvio acerca del correo basura, como opuesto a los virus u otros programas dañinos. Los que lo envían se dedican a eso para ganar dinero. Y quienes van detrás del dinero resultan ser criaturas relativamente fáciles de regular. Si el objetivo de la regulación actúa por dinero, entonces se puede controlar su conducta mediante la modificación de sus incentivos. Así, si ignorar una regulación sale más caro que obedecerla, entonces los remitentes de correo basura (tras pensárselo bien) la obedecerán. Tal obediencia puede significar modificar su conducta de envíos, o bien puede significar buscarse otro trabajo. De una u otra forma, basta con modificar los incentivos económicos para que cambie la conducta de envíos de correo basura.

Y ¿cómo modificar estos incentivos mediante la ley? ¿Existe alguna razón para creer que los remitentes de correo basura harán caso a la ley?

La gente se hace esas preguntas porque se percata muy razonablemente de que los Estados no dedican mucho tiempo a procesar a quienes envían correo basura. Y es que los Estados tienen mejores cosas que hacer (o eso creen). De este modo, ni siquiera una ley que criminalizara su actividad tendría una alta probabilidad de asustar a muchos de los que se dedican a este negocio.

Lo que necesitamos es más bien la clase de creatividad en la adaptación de la ley que los autores de código demuestran cuando construyen filtros de correo basura extraordinariamente sofisticados. Si resulta improbable que la ley tal como la aplica el Estado modifique los incentivos de los remitentes de correo basura, deberíamos hallar leyes que se apliquen de un modo que éstos teman.

Una de estas innovaciones sería un sistema de recompensas bien regulado. La ley exigiría que se marcase el correo basura con una etiqueta, he ahí el único requisito. Pero el castigo por no hacerlo sería, o bien el procesamiento por parte del Estado, o bien el procesamiento mediante un sistema de recompensas. La Comisión Federal de Comercio fijaría una cifra tal que lograra reclutar a un número suficiente de cazarrecompensas, los cuales tendrían derecho a la recompensa si fueran los primeros, o estuvieran entre los cinco primeros, en identificar a una parte responsable asociada con el correo electrónico infractor.

Pero ¿cómo la identificaría el cazarrecompensas? Bueno, lo primero sería determinar si se ha incumplido la regulación. La respuesta a esta pregunta se compone de una parte fácil y de otra más compleja. Si el correo lleva la etiqueta correspondiente es fácil de saber, pero si se trata o no de correo comercial inducirá un juicio más complejo.

Una vez que el cazarrecompensas esté convencido de que se ha infringido la regulación, él o ella deberá identificar a continuación una parte responsable. Y aquí la clave está en seguir una idea que el Senador John McCain introdujo en la única legislación sobre correo basura que el Congreso ha promulgado hasta la fecha, la Ley CAN-SPAM. Esa idea consistía en responsabilizar de la infracción tanto a la persona que envía el correo electrónico como a la entidad que se publicita en él.

En el 99 % de los casos, será prácticamente imposible identificar a quien envía el correo basura, ya que las técnicas que emplean estas personas para ocultar tal información son extremadamente sofisticadas.[66]

---

66 Véase Spammer-X, Jeffrey Polsuns y Stu Sjouwerman, *Inside the Spam Cartel: Trade Secrets from the Dark Side*, Nueva York, Syngress Publishing, 2004.

Ahora bien, identificar la entidad que se publicita en el correo basura es una cuestión diferente. De nuevo, si el correo basura quiere ser efectivo, debe incluir a alguien a quien pueda dar mi dinero. Si me resulta demasiado difícil dárselo, entonces ese correo no proporcionará el dinero necesario para ser rentable.

Entonces, ¿cómo puedo seguir la pista a la entidad que se publicita en el correo basura?

En este punto acudiría en nuestra ayuda el mercado de las tarjetas de crédito. Imaginémonos una tarjeta de crédito —llamémosla la «tarjeta de crédito de cazarrecompensas»— que, al ser verificada, siempre fuera rechazada. Ahora bien, cuando se usara dicha tarjeta, se agregaría una marca especial a la transacción y su titular conseguiría un informe sobre la entidad que intentó efectuar el cargo. El único propósito de esta tarjeta sería destapar e identificar las conductas punibles. Las empresas de tarjetas de crédito podrían fijar un precio especial por ella, o cobrar por cada uso; algo ciertamente deberían cobrar para que les mereciera la pena proveer esta tarjeta. Pero con ella en sus manos, los cazarrecompensas podrían generar registros utilizables sobre la persona que intentó realizar el cobro y, con tal información, ya podrían reclamar su recompensa.

Pero ¿de qué modo se impide que la gente malévola tienda una trampa a alguien? Pongamos que yo odio a mi competidor, Ajax Cleaners, así que contrato a un remitente de correo basura para que inunde California de mensajes anunciando una promoción especial en su nombre. Abro una cuenta donde ingresar el dinero a Ajax, y a continuación uso mi tarjeta de crédito de cazarrecompensas para pillarle. Hecho esto, acudo a cobrar mi recompensa a la Comisión Federal de Comercio, y ésta impone a Ajax Cleaners una cuantiosa multa que la lleva a la quiebra.

He aquí una preocupación sustancial con respecto a cualquier sistema de recompensas, la cual puede también abordarse, no obstante, mediante un cálculo cuidadoso de los incentivos. Lo primero, obviamente, es que la regulación debería castigar ese fraude con la muerte (de acuerdo, no con la muerte, pero sí con una condena importante). Y segundo, cualquier persona o empresa acusada de violar este estatuto podría declarar, bajo juramento, que no contrató o encargó a ninguna entidad el envío de correo basura en su nombre. Si la compañía realiza tal declaración, quedaría exenta de responsabilidad; pero si se prueba que la declaración es falsa, se la castigaría con una pena muy severa —que incluiría la confiscación de activos tanto personales como de la compañía. A una persona o empresa que firmara por primera

vez una de estas declaraciones probablemente se le concedería el beneficio de la duda, pero a aquélla que lo hiciera más veces se la sometería a una investigación oficial. A esas alturas, el riesgo de ser descubiertos que afrontarían los remitentes de correo basura bastaría para que ya no le salieran rentables sus envíos.

También en este caso, pues, la solución se basa en una estrategia de combinación de modalidades. Una *ley* crea el incentivo para una determinada modificación del *código* del correo basura (ahora llega etiquetado). Esa ley se aplica mediante un complejo conjunto de incentivos relativos al *mercado* y a las *normas* —tanto el incentivo para convertirse en cazarrecompensas, que es a la vez financiero y normativo (la gente está convencida de que los remitentes de correo basura actúan mal), como el estímulo para producir tarjetas de crédito de cazarrecompensas. Si se ejecuta bien, esta combinación de modalidades modificaría los incentivos a los que se enfrentan los remitentes de correo basura. Y si se ejecuta bien, esta modificación podría bastar para obligar a la mayoría de ellos a buscarse otro trabajo.

Esta estrategia, por supuesto, tiene sus límites: no funcionará bien con los sitios extranjeros, ni tampoco con los remitentes de correo basura que tengan intereses ideológicos (o patológicos). Ahora bien, éstos podrían entonces convertirse en el objetivo de las soluciones basadas en el código que describí al comienzo. Una vez eliminada la inmensa mayoría del correo basura comercialmente racional, los casos anómalos pueden abordarse de forma más directa.

* * * *

Ésta ha sido una sección extensa pero que nos ha dejado algunas ideas importantes. La primera es referente a nuestra perspectiva: para afirmar que una regulación «recorta la libertad de expresión o de prensa», necesitamos un punto de comparación. Las regulaciones que he descrito en esta sección están diseñadas para restaurar la regulación efectiva del espacio real; en este sentido, a mi modo de ver, no «recortan» la libertad de expresión.

La segunda idea es que estos ejemplos demuestran cómo no hacer nada puede ser peor para los principios de libertad de expresión que regular dicha expresión. La consecuencia de que no exista ninguna regulación legal que encauce la pornografía es un estallido de código dañino para regularla. La consecuencia de que no exista ninguna regulación legal efectiva que se ocupe del correo basura es una explosión de código dañino que ha perjudicado al correo electrónico. En otras palabras, la inexistencia de leyes a veces genera código

dañino. Polk Wagner plantea la misma idea: «La ley y el software definen de forma conjunta la condición reguladora. Menos ley no significa necesariamente más libertad».[67] Dado que el código y la ley son reguladores (aunque de diferente tipo), deberíamos evitar la mala regulación, sea del tipo que sea.

La tercera idea que estos ejemplos ponen de manifiesto es que la regulación del ciberespacio consiste siempre en una estrategia de combinación de modalidades. No existe ninguna solución milagrosa —ya sea código de la Costa Este o de la Costa Oeste. En su lugar, hay una combinación de técnicas —modalidades que han de equilibrarse para alcanzar cierto fin regulador— que deben tener en cuenta la interacción entre los reguladores. La cuestión, tal y como Polk Wagner la describe, se basa en el equilibrio. Pero la ley tiene reservado el importante papel de apremiar a que esa combinación garantice el equilibrio que sea promovido por una determinada política.

En este ámbito, una regulación inteligente nos permitiría evitar la destructiva regulación basada en código que vendría a llenar el vacío regulador. Y esto, a su vez, redundaría en pro de los intereses de la libertad de expresión.

Regulaciones de la expresión: cultura libre

El tercer contexto en el que considerar la especial relevancia del ciberespacio para la libertad de expresión se deduce directamente del Capítulo 10. Tal y como describí, la interacción entre la arquitectura de la ley de derechos de autor y la arquitectura de las redes digitales produce una explosión de creatividad sujeta a copyright nunca antes contemplada por ningún legislador.

Los elementos de ese cambio son simples. La ley de copyright regula, como mínimo, las «copias», y las redes digitales funcionan haciendo «copias»: no hay modo alguno de usar una obra en un entorno digital sin copiarla. Por consiguiente, todos y cada uno de los usos de obras creativas en un entorno digital están sujetos, en teoría, al copyright.

---

67 R. Polk Wagner, «On Software Regulation», *Southern California Law Review*, núm. 78, 2005, pp. 457-516.

Esto supone un cambio radical con respecto a la vida en el espacio real. En éste existe una gran variedad de formas de «usar» una obra creativa sin conculcar la ley de copyright. Cuando contamos a los amigos un chiste que hemos escuchado, no se invoca la ley de copyright —no se efectúa ninguna «copia» y, con respecto a los amigos, no se da ninguna comunicación pública—; cuando le prestamos un libro a un amigo, ello no incumbe a la ley de copyright; cuando leemos un libro, la ley de copyright hace caso omiso. Prácticamente, la totalidad de usos ordinarios de la cultura que se dan en el espacio real están libres de la regulación de derechos de autor, la cual se orienta hacia los usos anómalos —como pueden ser la «edición» o la comunicación pública.

La brecha entre usos ordinarios y anómalos comenzó a cerrarse a medida que se democratizaron las tecnologías de copia. Xerox dio el pistoletazo de salida con sus fotocopiadoras; los grabadores de cintas de casette siguieron sus pasos poco después. Pero incluso estas tecnologías constituían la excepción, nunca la regla. Suscitaron interrogantes en torno al copyright, pero no lo incrustaron en el centro de la vida ordinaria.

Eso lo han hecho las tecnologías digitales. A medida que una proporción cada vez mayor de la vida ordinaria se desplaza a Internet, una proporción cada vez mayor de ella queda sujeta a copyright. El equivalente funcional de las actividades del espacio real que quedaban al margen de regulación está ahora sujeto a la regla del copyright en el ciberespacio. Aquella actividad creativa que nunca tuvo que bregar con la regulación de derechos de autor ahora debe, para ser legal, salvar innumerables obstáculos, algo que resulta imposible en algunos casos dado el sistema de propiedad desquiciadamente ineficaz que es el copyright. De resultas, una importante proporción de la actividad creativa ha pasado en la actualidad del ámbito de la cultura libre al de la cultura del permiso. Y la cuestión que concierne a los principios de la libertad de expresión es si debería permitirse la expansión sin cortapisas de tal regulación.

Una vez más, yo tengo mis propias ideas (demasiado intensas) al respecto.[68] No deja de asombrarme que un Tribunal Supremo tan ansioso por evitar «aumentar los costes de los productores de materiales sexuales turbadores para la mayoría»[69] se mantenga aparentemente ajeno al modo en que la ley de copyright aumenta los costes de ser productor de expresiones creativas y críticas.

---

68 Lessig, *Free Culture: The Nature and Future of Creativity*, *op. cit.*, pp. xiii-xvi.

69 Yochai Benkler, «Net Regulation: Taking Stock and Looking Forward», *University of Colorado Law Review*, núm. 71, 2000, pp. 1203-1249.

Pero para nuestra finalidad aquí, deberíamos simplemente advertir una vez más una ambigüedad latente en nuestra tradición constitucional. Tal y como ha sostenido el Tribunal Supremo, la Primera Enmienda impone limitaciones importantes sobre el alcance del copyright. Entre ellas figuran al menos los requisitos de que el copyright no regule «ideas» y de que esté siempre sujeto al «uso justo».

Ahora bien, estas «salvaguardas tradicionales de la Primera Enmienda» se desarrollaron en un contexto donde el copyright constituía la excepción, no la regla. Aún no poseemos una tradición en la que todos y cada uno de los usos de obras creativas estén sujetos a copyright. Las tecnologías digitales han producido ese mundo, pero la mayor parte del resto del mundo todavía no se ha dado cuenta.

Así pues, ¿cuáles deberían ser los principios de la Primera Enmienda en este mundo? Un punto de vista es que la Primera Enmienda no debería desempeñar ningún papel —más allá de las protecciones mínimas de la distinción entre «idea» y «expresión» y del requisito del «uso justo». Desde esta perspectiva, el alcance de la regulación del Congreso sobre las actividades creativas es, respetando esas condiciones mínimas, pleno. Cualquier acto creativo reducido a una forma tangible podría quedar sujeto al derecho monopolístico que establece el copyright; y como todo acto creativo en un contexto digital se reduce a una forma tangible, este punto de vista implica que en el mundo digital todo podría someterse al copyright.

El punto de vista contrario rechaza este alcance ilimitado del copyright. Mientras que el derecho monopolístico del copyright tiene sentido en ciertos contextos comerciales, o más claramente, tiene sentido allá donde es necesario «promover [...] el progreso», no hay razón legítima alguna para imponer a la inmensa mayoría de la expresión creativa los gravámenes de la ley de copyright. Que un niño que graba un reportaje de video sobre un libro necesite obtener los permisos correspondientes del autor, o que los amigos que realizan una versión de su artista favorito no puedan hacerlo a menos que su sello discográfico les haya concedido permiso, extiende el alcance del copyright más allá de cualquier propósito legítimo.

Lo que está claro, no obstante, es que los redactores de la Constitución nunca llegaron a optar entre estos dos puntos de vista. Y es que ellos nunca se enfrentaron a la opción de que el copyright pudiera (eficazmente) controlar todos y cada uno de los usos de las obras creativas. Allá por 1790, cualquier posible control de este tipo habría resultado radical y excesivamente oneroso. Y aunque yo apostaría acerca del sentido de su voto, dada su firme

aversión a los monopolios y dada la cláusula de propiedad intelectual tan restrictiva que promulgaron, esto no deja de ser una simple apuesta. Si en este ámbito hay que tomar una decisión, ellos no lo hicieron. Somos nosotros, entonces, los que hemos de decidir si los principios de libertad de expresión restringen esta extensión radical del alcance de la regulación de copyright.

Los reguladores de la expresión: distribución

Hasta ahora mi argumentación en torno a la arquitectura se ha referido a las arquitecturas en el ciberespacio, pero en esta historia final me dispongo a difuminar un poco las fronteras. Deseo usar la arquitectura del ciberespacio para demostrar algo importante sobre la regulación de la radiodifusión.

La Comisión Federal de Comunicaciones regula la expresión. Si yo quisiera emitir un discurso político a través de una emisora FM en la frecuencia de 98.6 MHz de San Francisco, la FCC me procesaría.[70] Para hablar en esa frecuencia de San Francisco, necesito una licencia, ya que usar estas radiofrecuencias sin una licencia constituye un delito; y esto a pesar de que la Constitución establece que el «Congreso no hará ninguna ley [...] que recorte la libertad de expresión o de prensa». ¿Qué pasa aquí?

La respuesta a esta pregunta se basa en una asunción profundamente arraigada en el núcleo de nuestra jurisprudencia relativa a las tecnologías de radiodifusión: sólo se dispone de una cantidad fija de «espectro» de radiofrecuencia, y la única manera de facilitar su empleo es asignar fracciones de dicho espectro a los usuarios, que tendrán entonces derecho a utilizarlas dentro de una región geográfica concreta. Sin tal asignación, la radiodifusión sería un caos, y este caos acabaría matándola.

Esta idea apareció por primera vez en la escena constitucional después de que el Congreso promulgara la Ley de Radio de 1927.[71] Un año antes, Herbert Hoover, secretario de Comercio, abandonó la práctica de controlar

---

70 Véase, por ejemplo, *United States vs. Dunifer*, 219 F.3d 1004, 9º Cir., 2000 (cierre de la FCC de la emisora de radio pirata *Free Radio Berkeley*); *United States vs. Any & All Radio Station Transmission Equip.*, 2004 U.S. Dist. LEXIS 24899, DNY, 2004; *United States vs. Szoka*, 260 F3d 516, 6º Cir., 2001. Véase 47 CFR 73.277, 1998.

71 47 USCA 81–119, 1927; derogada por la Ley de Comunicaciones de 1934.

la radiodifusión después de que un buen número de tribunales le denegaran el poder para hacerlo. Si él no tenía tal poder, alegó Hoover, entonces la mano invisible tendría que gobernar el espectro. Pero como no era muy amigo de la mano invisible, Hoover predijo lo que sobrevendría cuando se le retiraran las competencias —el caos. Hay quien sugiere que su objetivo era contribuir a que ocurriera precisamente lo que predijo, esto es, que unas emisoras de radio se solaparan con otras y que la radiodifusión fuera un desastre. Así, en el momento en que surgió alguna confusión, Hoover la utilizó para justificar la introducción de nuevas leyes federales.[72]

Entonces el Congreso acudió al rescate, autorizando a la FCC a regular el espectro de una manera ampliamente invasiva. Sólo quienes tuviesen una licencia podrían hablar; lo que dijesen estaría controlado mediante su licencia; debían hablar en interés público y compartir sus recursos con sus competidores. En resumen, el Congreso estableció que la radiodifusión tenía que regularse de la misma forma que la Unión Soviética regulaba el trigo.[73] No había elección. Como afirmó el juez Felix Frankfurter al ratificar este régimen, tal *sovietismo* venía impuesto por la «naturaleza» de la radio.[74]

Desde el principio, no obstante, ha habido escépticos con respecto a esta idea —no escépticos con respecto a la idea de que el espectro debe ser regulado, sino con respecto a la manera de hacerlo. ¿Es realmente necesario tener una agencia central que asigne lo que en realidad son derechos de propiedad? Tal y como argumentaron estos escépticos, el derecho consuetudinario había desempeñado bien esas funciones antes de que las asumiera el gobierno federal; podría seguir haciéndolo simplemente si dicho gobierno convirtiera el espectro en un tipo de derecho de propiedad intercambiable. En 1959 adquirió gran resonancia la propuesta de Ronald Coase de un régimen en que se otorgase el espectro mediante subasta en vez de mediante licencia.[75] La idea de Coase acabó imponiéndose —cincuenta años después.

---

72 Véase *Red Lion Broadcasting Company vs. Federal Communications Commission,* 395 US 367, 375–77, 1969; *National Broadcasting Company vs. United States,* 319 US 190, 212–13, 1943. Thomas Hazlett critica rotundamente la historia de Frankfurter sobre la emergencia de cualquier necesidad de regulación por parte de la FCC; véase Thomas W. Hazlett, «Physical Scarcity, Rent Seeking, and the First Amendment», *Columbia Law Review*, núm. 97, 1997, pp. 905, 933–934.

73 Véase *Turner Broadcasting System, Inc. vs Federal Communications Commission*, 512 US 622, 637–38, 1997; véase también Huber, *Law and Disorder in Cyberspace, op. cit*.

74 Véase *National Broadcasting Company, Inc. vs. Columbia Broadcasting System*, p. 213.

75 Véase Ronald H. Coase, «The Federal Communications Commission», *Journal of Law and Economics*, núm. 2, 1959, p. 1.

Así, en la actualidad, la FCC subasta enormes franjas del espectro de radiofrecuencia estadounidense, y en el momento de escribir este libro, se estaba posicionando para vender un espectro electromagnético de gran importancia —la parte que se utilizaba para emitir televisión en UHF.

En cualquiera de los dos escenarios —en el que la FCC asigna franjas del espectro o en el que concede derechos de propiedad sobre él—, el Estado se reserva un papel. En el primer caso, dicho papel tiene máximo protagonismo, ya que la FCC debe decidir a quién concede sus licencias. En el segundo caso, la FCC sólo necesita aplicar los límites que establece el derecho de propiedad. En cierta forma, esta última es una forma de gobierno menos inquietante que la primera, en la que el Estado decide a quién prefiere.

En todo caso, ambas formas de regulación producen una «prensa» (al menos la prensa que utiliza el espectro) que difiere mucho de la «prensa» que conocieron los redactores de la Constitución estadounidense. En 1791 la «prensa» no estaba conformada por cabeceras como *The New York Times* o *The Wall Street Journal*. En efecto, la prensa de entonces no se componía de grandes organizaciones de intereses privados, con millones de lectores asociados a cada organización. Más bien al contrario, la prensa en aquel entonces se parecía mucho a la Internet actual. El coste de una imprenta era bajo, el número de lectores también, el Estado subvencionaba su distribución y cualquier persona podía (dentro de lo que cabe) convertirse en editor. Muchos lo hicieron.[76]

En cambio, las licencias y los derechos de propiedad sobre el espectro de radiofrecuencia producen un mercado totalmente diferente. El coste derivado de obtener una u otra concesión se convierte en una barrera de entrada, como una regla que exigiera una «licencia de periódico» para publicar uno. Si tal licencia resultase cara, menos gente podría lanzar su diario.[77]

Por supuesto, en virtud de la Primera Enmienda sería imposible imaginarse al Estado otorgando licencias para editar periódicos (al menos si esa licencia resultase cara y se dirigiera al sector de la prensa). Y esto porque todos compartimos la firme intuición de que es deseable que sea la competencia,

---

76 Paul Starr, *The Creation of Media: Political Origins of Modern Communications*, Nueva York, Basic Books, 2004, pp. 25–46.

77 Yochai Benkler, «Net Regulation: Taking Stock and Looking Forward», *University of Colorado Law Review*, núm. 71, 2000, p. 1203.

y no las barreras estatales artificiales, la que determine qué periódicos pueden operar; y porque todos sabemos intuitivamente que no hay necesidad alguna de que el Estado «racionalice» el mercado de los periódicos. La gente es capaz de elegir entre los distintos diarios sin ayuda del Estado.

¿Y si lo mismo fuera cierto para el espectro de radiofrecuencia? La mayoría de nosotros no tiene ni idea de cómo funciona lo que llamamos «espectro». Los extraños sonidos y la recepción inestable de nuestras radios FM y AM nos empujan a atribuir a cierta magia especial lo que sucede entre la emisora y nuestro aparato receptor. Sin tal magia, las ondas de radio «interferirían» las unas con las otras. Se entiende que es necesaria una cierta coordinación especial para evitar tal «colisión» y el inevitable caos que resultaría de ella. Desde esta perspectiva, las ondas de radio son delicados aviones invisibles que necesitan a celosos controladores de tráfico aéreo para cerciorarse de que no se produzca el desastre.

Pero lo que la mayoría de nosotros cree saber acerca de la radio es erróneo. Las ondas no son mariposas y tampoco necesitan la protección de burócratas federales para llegar hasta nuestro receptor. Y como demuestra la tecnología con la que todos los internautas estarán familiarizados, *ni* las licencias *ni* los derechos de propiedad sobre el espectro tienen realmente razón de ser. En este contexto, la mano invisible puede hacer todo el trabajo.

Para captar el porqué de esta afirmación, consideremos dos contextos, uno de los cuales es conocido por todo el mundo. Sin duda, las ondas de radio son diferentes de las ondas de sonido, pero, para nuestro propósito aquí, la siguiente analogía sirve muy bien.

Imaginémonos que estamos en una fiesta. Hay cincuenta personas en la sala y todas ellas están hablando, es decir, todas están produciendo ondas sonoras. Ahora bien, aunque cada uno de estos interlocutores produce diferentes ondas sonoras, no tenemos ninguna dificultad para escuchar a la persona que está a nuestro lado. Con tal de que nadie se ponga a gritar, podemos arreglárnoslas bien para oír la conversación en la que estamos inmersos. De forma más general, una fiesta se compone (al principio de la noche al menos) de interlocutores perspicaces que coordinan sus intervenciones de forma que la práctica totalidad de los asistentes puede comunicarse sin dificultad alguna.

Las radios podrían funcionar de un modo similar —si el receptor y el emisor fueran análogamente inteligentes. En lugar de los aparatos receptores «tontos» en los que se apoyan las emisiones en FM o AM, las radios

inteligentes podrían modular la recepción y la comunicación del mismo modo en que los asistentes a una fiesta se concentran en la conversación que están manteniendo.

La mejor prueba de ello la constituye el segundo ejemplo que ofrezco para refutar la interpretación común acerca del funcionamiento del espectro. Este ejemplo se llama *wifi*. *Wifi* es el nombre popular de un conjunto específico de protocolos que conjuntamente permiten que los ordenadores «compartan» bandas de espectro libre de licencias, entre las cuales la más popular es la que ocupa la franja 2.5 GHz—5 Ghz. La tecnología *wifi* permite a una gran cantidad de ordenadores emplear dicho espectro para comunicarse.

Sin duda la mayoría de lectores de este libro habrá tenido contacto con esta tecnología. Yo me la encuentro todos los días que tengo clase: un aula repleta de estudiantes que, equipados con sus respectivos portátiles, se conectan en su inmensa mayoría a Internet —haciendo quién sabe qué. Los protocolos incluidos en sus ordenadores les permiten a todos ellos «compartir» una reducida banda de espectro. Ningún Estado o regulador indica a cada ordenador cuándo puede emitir, como tampoco los necesitamos para asegurarnos de que los asistentes a un cóctel pueden comunicarse entre sí.

Estos ejemplos son, por supuesto, pequeños y limitados. Pero hay literalmente toda una industria dedicada actualmente a difundir lo que nos enseña esta tecnología de la forma más extensa posible. Algunos teóricos creen que el uso más eficaz de todo el espectro se basaría en estos modelos —empleando tecnologías de banda ultra-ancha[78] para maximizar la capacidad del espectro de radio. Pero incluso los escépticos sobre esta utopía del espectro empiezan a comprender que nuestras asunciones sobre cómo debe asignarse éste se fundan sobre la ignorancia acerca de su funcionamiento real.

El ejemplo más claro de esta falsa asunción es el conjunto de intuiciones que probablemente tengamos sobre las limitaciones necesarias en la utilización del espectro. Tales asunciones vienen respaldadas, además, por la idea de la propiedad del espectro. La imagen que probablemente tenemos es la de un recurso que puede llegar a ser esquilmado. Así, al igual que demasiado ganado puede esquilmar un pasto, pensamos que demasiados usuarios pueden llegar a saturar los canales.

---

78 La FCC define como banda ultra-ancha (*ultra-wide-band*) aquella tecnología de radio que emplea un ancho de banda superior a 500 MHz o al 25 % de la frecuencia central. [N. del E.]

Ciertamente la congestión es una consecuencia posible del uso del espectro. Pero el aspecto crucial que hemos de reconocer —aspecto que, de nuevo, resuena a lo largo de todo este libro— es que esta posibilidad de congestión depende del diseño de las redes. Las redes *wifi* ciertamente pueden llegar a congestionarse, pero una arquitectura diferente de «compartición» del espectro no tiene por qué hacerlo. De hecho, según este diseño, el aumento de usuarios no merma la capacidad de la red, sino que la incrementa.[79]

La clave para hacer posible este sistema consiste en que cada receptor se convierta en un nodo dentro de la arquitectura del espectro. Los usuarios no serían entonces meros receptores de una transmisión ajena, sino que se convertirían también en emisores. Del mismo modo que las tecnologías P2P como BitTorrent aprovechan el ancho de banda de sus usuarios para compartir el coste de distribución del contenido, los usuarios de una determinada arquitectura de espectro de red de malla [*mesh network*] podrían realmente aumentar la capacidad de espectro de dicha red. Según este diseño, pues, cuanta más gente use el espectro, más espectro estará disponible para uso de los demás —produciendo no una tragedia, sino una comedia del procomún.[80]

La arquitectura básica de este sistema de malla concibe cada ordenador conectado a él como receptor y como emisor a la vez. Por supuesto, en cierto sentido, eso es lo que estas máquinas ya son —un ordenador conectado

---

79 Véase, por ejemplo, la investigación del MIT para construir redes de malla virales cuya capacidad se incrementa a medida que aumentan los usuarios. «Collaborative (Viral)Wireless Networks», disponible en http://web.media.mit.edu/~aggelos/viral.html.

80 El autor efectúa aquí un juego de palabras alusivo a la expresión acuñada por el biólogo Garrett Hardin en su influyente artículo «The Tragedy of the Commons» («La Tragedia del Procomún»), publicado en 1968 en la revista *Science* (disponible en http://www.sciencemag.org/cgi/content/full/162/3859/1243). En él, Gardin ilustra este concepto a través del ejemplo de un pasto explotado de forma comunal por varios ganaderos. Así, el autor explica que cada ganadero, en cuanto ser racional, buscará maximizar sus beneficios llevando a pastar allí todo el ganado que pueda. Ello le reportará un beneficio individual pero irá esquilmando cada vez más el pasto, dado que el resto de ganaderos aplicará la misma lógica: «He ahí la tragedia. Todos los hombres están atrapados dentro de un sistema que les compele a incrementar su ganado de forma ilimitada —en un mundo que es limitado. La ruina es el destino hacia el que se precipitan todos ellos, cada cual persiguiendo su propio interés en una sociedad que cree en la libertad del procomún» (*ibidem*, p. 1244).

Por su parte, la expresión «La Comedia del Procomún» ha servido de título a un conocido artículo de Carol M. Rose («The Comedy of the Commons: Commerce, Custom and Inherently Public Property», *University of Chicago Law Review*, núm. 53, 1986, pp. 711-781), además de a una célebre conferencia que el propio Lessig pronunció el 23 de septiembre de 2004 (disponible para su escucha y descarga en http://itc.conversationsnetwork.org/shows/detail349.html) [N. del E.].

a una red *wifi* recibe y envía transmisiones al nodo de radiodifusión. Ahora bien, esa arquitectura responde al esquema de difusión masiva, del que difiere la arquitectura de malla. En ella, cada radio puede enviar paquetes de datos a cualquier otra radio dentro de dicha red; o, expresado de otra forma, cada radio es un nodo de la red, cuya capacidad podría crecer con la incorporación de nuevos nodos. En cierto sentido, ésta es precisamente la arquitectura de buena parte de Internet. Los ordenadores tienen direcciones donde recopilan paquetes enviados a ese ordenador desde la red.[81] Así, nuestro ordenador comparte la red con todos los demás. Internet posee un protocolo para compartir este procomún; una vez que se establece el protocolo, no se necesita más regulación.

No hemos de profundizar demasiado en esta tecnología para reconocer la cuestión que pretendo que se plantee en esta sección: si la tecnología posibilita que las radios compartan el espectro —prescindiendo de licencias y derechos de propiedad—, ¿qué justificación tiene el Estado para imponer uno u otro gravamen al uso del espectro? O, para enlazar con el comienzo de esta sección, si los usuarios del espectro pudieran compartirlo sin que medie coordinación estatal, ¿por qué está más justificado que el Estado imponga un sistema de propiedad sobre el espectro de lo que lo está que cobre a los periódicos por el derecho a la publicación?

Sin duda, la arquitectura que posibilita la compartición no está totalmente libre de regulación estatal. El Estado podría exigir que sólo se usen dispositivos certificados en esta red (como ya hace la FCC con cualquier dispositivo que pueda irradiar dentro de una franja del espectro); podría impulsar la capacidad de esta tecnología, incrementando la arquitectura de malla; incluso podría imponer razonablemente límites enojosos a la potencia de cualquier transmisor. Pero más allá de estas sencillas regulaciones, el Estado no debería limitar quién accede al espectro ni prohibir su uso a quienes no hubieran pagado u obtenido una licencia.

Así pues, nos encontramos aquí con dos arquitecturas para el espectro —una en la que éste es asignado, y otra en la que es compartido (como el mercado de los periódicos). ¿Cuál de ellas es más coherente con el designio de la Primera Enmienda?

---

81 Así funciona efectivamente el estándar ethernet. Los datos de una red ethernet fluyen a todos los ordenadores conectados a ella, cada ordenador olfatea los datos y luego presta atención a los dirigidos a él. Este proceso crea un agujero de seguridad obvio: los «olfateadores» pueden configurarse en «modo promiscuo», de modo que lean paquetes dirigidos a otras máquinas; veáse Loshin, *TCP/IP Clearly Explained, op. cit.*, pp. 44–46.

He aquí, finalmente, un ejemplo de traducción que funciona. Hemos de elegir entre una arquitectura que es el equivalente funcional de la arquitectura del modelo constitucional estadounidense, y otra equivalente al modelo soviético. Una arquitectura distribuye el poder y facilita la expresión, mientras que la otra concentra el poder y aumenta los costes de expresarse. En este caso, los redactores optaron claramente por uno de los dos esquemas. El Estado no debe intervenir ni directa ni indirectamente en la concesión de licencias a los emisores, por más que eso sea precisamente lo que permite la actual regulación de asignación del espectro.

Mi colega Yochai Benkler y yo hemos defendido[82] que una interpretación fidedigna de la Constitución implicaría la liquidación del régimen de asignación del espectro.[83] Tal interpretación rechazaría una arquitectura que propiciara tamaña concentración de poder. El modelo de expresión que los redactores de la Constitución adoptaron coincide exactamente con el modelo de Internet —distribuida, descentralizada, completamente libre y diversa. Por supuesto, a nosotros nos correspondería elegir si queremos una lectura fidedigna —la traducción no proporciona su propio respaldo normativo. Ahora bien, si nuestro objetivo es la fidelidad, la respuesta es ésta.

Lecciones sobre la expresión

Lo que al principio de este libro describí como modalidades de restricción lo he descrito en este capítulo como modalidades de protección. Mientras que las modalidades de restricción pueden usarse como espadas contra el individuo (poderes), las modalidades de protección pueden usarse como escudos (derechos).

---

82 Véase Yochai Benkler y Lawrence Lessig, «Net Gains», *New Republic,* 14 de diciembre de 1998.

83 El «fundador» de este argumento ha de ser Eli Noam; véase «Spectrum Auctions: Yesterday's Heresy, Today's Orthodoxy, Tomorrow's Anachronism —Taking the Next Step to Open Spectrum Access», *Journal of Law and Economics*, núm. 41, 1998, p. 765. Benkler lo ha aderezado un poco (a mi entender, de forma crucial) añadiéndole el valor del procomún. Para una reivindicación extraordinariamente potente de un objetivo político (si no tecnológico) similar, véase Eben Moglen, «The Invisible Barbecue», *Columbia Law Review*, núm. 97, 1997, p. 945. Moglen observa la ausencia de debate respecto a las consecuencias sociopolíticas de cercenar los derechos referentes a las telecomunicaciones en la «Gran Barbacoa», y establece un paralelismo con la asignación de beneficios y privilegios de la industria ferroviaria en la Era Dorada de EEUU.

En principio, podríamos reflexionar acerca del modo en que estas cuatro modalidades protegen la expresión, pero aquí yo me he centrado en las arquitecturas, preguntándome: ¿qué arquitecturas protegen qué tipos de expresión? ¿De qué modo una modificación arquitectónica modifica el tipo de expresión que se protege?

No he intentado ofrecer una visión exhaustiva al respecto; ahora bien, he defendido un punto de vista que aborda integralmente la relación entre arquitecturas y expresión, y que se apoya en principios constitucionales para reflexionar no sólo sobre lo que está permitido dada una arquitectura concreta, sino también sobre qué arquitecturas están permitidas. Nuestra constitución del espacio real debería informar los principios de nuestra constitución del ciberespacio; o al menos debería impedir los esfuerzos del Estado por imponer en el ciberespacio una arquitectura totalmente incongruente con dichos principios.

13. Interludio

Detengámonos un instante para echar la vista atrás sobre los tres últimos capítulos. Existe una pauta para los problemas que presentan —un modo de comprender cómo esos tres problemas son en realidad uno solo.

En cierto sentido, cada uno de ellos ha planteado el interrogante: ¿cuánto control sobre la información deberíamos permitir, y quién debería ejercerlo? Hay una batalla entre el código que protege la propiedad intelectual y el uso justo; hay una batalla entre el código que podría generar un mercado en torno a la privacidad y el derecho a desvelar datos sobre los individuos al margen de ese mercado; hay una batalla entre el código que permite filtros perfectos de la expresión y las arquitecturas que garantizan cierto desorden sobre quién accede a qué información. Cada caso exige alcanzar un equilibrio en el control.

Puede que parezca que mi voto varía en cada contexto. En lo que concierne a la propiedad intelectual, he argumentado en contra del código que realiza un seguimiento de la lectura y a favor del código que garantiza un amplio espacio para el procomún intelectual. En el contexto de la privacidad, he argumentado a favor del código que permite la decisión individual —tanto para cifrar como para expresar preferencias sobre qué datos personales son susceptibles de ser recopilados por otros. El código permitiría tomar esa decisión y la ley podría inspirar dicho código. En el contexto de la libertad de expresión, sin embargo, he argumentado en contra del código que establezca filtros perfectos a la expresión —defendiendo que resulta demasiado peligroso permitir la elección perfecta en este ámbito. Por supuesto, perfeccionar las elecciones siempre es mejor, por lo que un código que potencie mejores estructuras de autoridad será bueno, como también lo será un código que amplíe el espectro legítimo de radiodifusión.

El objetivo en cada uno de estos tres contextos es impugnar las estructuras centralizadas de decisión. En el contexto de los filtros, sin embargo, el objetivo es impugnar también las estructuras demasiado individualizadas.

El lector podría preguntarme si estas opciones son coherentes. Yo pienso que sí, pero lo importante no es que esté de acuerdo conmigo. Puede que el lector crea que un equilibrio diferente también tendría sentido —acaso más control sobre la propiedad intelectual o los filtros, y menos sobre la privacidad. Lo que de verdad me interesa es transmitir la necesidad de tal equilibrio y de los principios implícitos en la reivindicación de que siempre necesitaremos un equilibrio. Siempre se da una competencia entre lo público y lo privado; siempre han de equilibrarse los derechos privados con los intereses públicos. Siempre ha de tomarse una decisión acerca de hasta dónde permitiremos llegar a cada parte. Estas preguntas son inherentes al Derecho Público: ¿cómo se sopesará una constelación específica de principios constitucionales? ¿Cómo podrá hallarse un equilibrio en contextos concretos específicos?

He sostenido esta idea al tiempo que evitaba especificar quién es responsable de cada desequilibrio dado. Hay quienes afirmarían que existen demasiados filtros, no suficiente privacidad o demasiado control sobre la propiedad intelectual, pero que ello no constituye un asunto de interés público, a menos que el Estado sea responsable de dichos desequilibrios. En EEUU los principios constitucionales llegan hasta donde llega la acción estatal. Y yo no he mostrado cómo la acción estatal se extiende a estos contextos.

Tampoco lo pretendo. En mi opinión, nuestra tradición revela al menos una ambigüedad sobre lo lejos que han de llegar los principios constitucionales. En un mundo donde el único regulador es el Estado, tiene cierto sentido limitar la autoridad de la Constitución a la acción estatal. Pero cuando las modalidades de regulación se multiplican, no hay ninguna razón para ignorar el alcance de los principios constitucionales. Los redactores de la Constitución estadounidense no tomaron una decisión a este respecto; no hay ninguna razón por la que la regulación mediante el código no pueda venir informada por los principios constitucionales. No se ha expuesto ningún argumento que defienda por qué esta parte de nuestra vida debería quedar al margen de las limitaciones y protecciones tradicionalmente proporcionadas por la Constitución.

El código establece el equilibrio entre derechos individuales y colectivos que he destacado hasta ahora. El próximo capítulo analiza un equilibrio diferente —uno que de nuevo es puesto de relieve por el código. No obstante, esta vez no se trata del equilibrio entre el Estado y el individuo sino entre

el Estado y las regulaciones implícitas de las arquitecturas del ciberespacio. En esta ocasión, la amenaza se cierne sobre una soberanía tradicional. ¿Cómo traducimos esa tradición para que encaje en un mundo donde el código es la ley?

Cuarta parte

Soberanos en competencia

Los soberanos se toman a sí mismos muy en serio —especialmente los del ciberespacio. Todos poseen un sentido muy marcado de sus respectivos dominios, y a veces tal sentido se traduce en dominación sobre otros campos. A medida que cada vez más soberanos se trasladan a la red, las reclamaciones de unos de controlar la expresión o la conducta entrarán progresivamente en conflicto con las de otros. Tal conflicto demostrará ser el hecho generativo más importante de la Internet que viene.

En las próximas páginas, abordaré este conflicto en dos pasos. El primer capítulo de esta Cuarta Parte trata la cuestión de la soberanía, independientemente del mencionado conflicto. ¿Qué significa la soberanía? ¿Cómo se manifiesta? A partir de aquí, el siguiente capítulo se centra en la dinámica particular que va a crear el conflicto entre soberanías. A mi juicio, tal conflicto empujará la arquitectura de Internet a un tipo de forma que nos resulta familiar.

14. Soberanía

Vietnam es una nación comunista, una de las pocas que quedan. Por supuesto, el tipo de comunismo que impera en ella no tiene nada que ver con el que dio nacimiento a la Guerra Fría. Pese a todo, Vietnam es una nación soberana que aún vincula su identidad a Marx y Lenin (a través del presidente Ho).

EEUU no es una nación comunista. Derrotada por Vietnam, pero vencedora de la Guerra Fría, es una nación que, en buena medida, se define en oposición a la ideología de Marx y Lenin. Vietnam defiende como ideal poner el Estado al servicio de un Estado decadente, mientras que EEUU defiende como ideal poner un Estado decadente al servicio de la libertad. El control constituye el modelo del comunismo; la libertad, el modelo de EEUU.

O eso es lo que creemos.

Confieso que los Estados comunistas me provocan cierta fascinación. A principios de la década de los años ochenta, deambulé por todos los países comunistas que me permitieron la entrada en su territorio; a comienzos de la siguiente década, colaboré con los constitucionalistas de Georgia mientras redactaban el anteproyecto de su Constitución; y pasé buena parte del verano de 1996 vagando por Vietnam. Solo y libre del correo electrónico, traté de comprender aquel lugar que, en mi niñez, fue víctima de la Guerra Fría exportada por mi nación.

Pese a que he estado en numerosos lugares diferentes del mundo, nunca he visitado uno tan espectacular como Vietnam. Uno siempre se siente abrumado por el perdón, y un estadounidense no puede evitar sentirse así ante

la calurosa bienvenida que se le dispensa en esta nación. Acaso si EEUU hubiese «ganado» la guerra, dicha indulgencia no se mostraría tan ostensiblemente. Pero, en apariencia, perdonar les resulta fácil a los vencedores.

Sea como fuere, yo no estaba allí para comprender la clemencia de los vietnamitas, sino para aprender cómo funcionaba su sistema político. Deseaba comprender cómo el Estado vietnamita ejerce el control sobre sus ciudadanos; cómo continúa regulando; en qué sentido se lo califica como uno de los últimos Estados comunistas que quedan en el mundo. Así que dediqué tiempo a charlar con abogados, hombres de negocios y directores de la emergente Red de Vietnam (NetNam). Muy pronto, surgió un panorama sorprendente.

Aunque la ideología de un Estado comunista admite muy poca limitación al poder estatal; aunque el Estado vietnamita antepone como ideal el bien común al bien o a la libertad individuales; aunque sobre el papel no hay «libertad» en Vietnam en el sentido en que nos gusta imaginarla en Occidente — aunque todo esto es verdad, no podía eludir el sentimiento de que la gente de Vietnam, en su existencia cotidiana, estaba mucho menos «regulada» que la de EEUU.

No toda la gente, por supuesto: los opositores políticos, indudablemente, sienten sobre ellos todo el poder del Estado. Pero me dio la sensación de que, en su vida cotidiana, las personas corrientes, muchas de ellas dueñas de pequeñas tiendas, no tenían ninguna concepción del control que puede ejercer el Estado; tampoco ninguna experiencia de remitir informes contables trimestrales a una burocracia central; y tampoco ninguna comprensión de lo que es vivir bajo la eficacia (relativa) de la regulación que se da en EEUU. La vida allí se desarrolla con extraordinaria libertad respecto al control estatal. Y resultaba difícil imaginarse que ello habría cambiado si Nixon hubiera ganado la guerra. La pornografía estaba prohibida y los *hippies* eran acosados, pero, en general, la gente y los negocios se desenvolvían sin apenas interferencia de una regulación estatal directa o eficaz.

Este hecho (si el lector admite que se califique como tal las observaciones aleatorias de un antropólogo desentrenado) no es difícil de comprender. La «ley» recogida en los libros de Vietnam puede ser o no un regulador más estricto o más amplio que la «ley» de EEUU, pero la arquitectura de la vida en Vietnam claramente imposibilita cualquier regulación real por parte del Estado. No existe una infraestructura de control —de hecho, apenas existe infraestructura de ninguna clase. Sean cuales sean las regulaciones estatales, no existe una arquitectura que pueda hacerlas efectivas. Incluso si allí hay más regulación que en EEUU (y, francamente, dudo que la haya), Vietnam goza de una «libertad» efectiva.

Esto tiene pleno sentido. El poder de regulación es una función de la arquitectura tanto como de la ideología; las arquitecturas permiten la regulación del mismo modo que la restringen. Para comprender el poder que un Estado puede tener, hemos de comprender las arquitecturas en el seno de las cuales gobierna.

Todos los capítulos anteriores han girado en torno a esta cuestión. Podemos hacernos una idea acerca del poder de una soberanía —del poder del soberano para regular o controlar la conducta—, pero la relevancia de ese poder se materializa en un contexto específico. El poder estatal puede ser «absoluto», pero si la arquitectura no respalda la regulación, en la práctica el poder del Estado se ve bastante mermado. Por otro lado, el poder estatal puede ser limitado, pero si las arquitecturas de control son muy eficaces, tal poder limitado puede ser extraordinariamente amplio. Por consiguiente, para comprender el poder regulador de un Estado hemos de preguntar: ¿en qué medida su infraestructura respalda la regulación?

He aquí la pregunta que deberíamos formular acerca del ciberespacio, como un primer paso para comprender la soberanía allí. ¿Qué poder poseen los soberanos para regular la vida en el ciberespacio? ¿Cómo respaldan o limitan ese poder las distintas modalidades de regulación?

Abordaremos esta cuestión en tres partes, dos de las cuales constituyen el eje de este capítulo. En primer lugar, ¿cuál es la naturaleza de la soberanía en el ciberespacio? ¿En qué se diferencia de la soberanía de Francia? En segundo lugar, ¿qué limita la soberanía del ciberespacio? Y en tercer lugar, lo que constituye el tema de la siguiente sección, ¿cómo interactuarán los soberanos en la regulación del ciberespacio, no tanto para controlar la conducta *allí* sino para controlar sus efectos *aquí*? ¿Cómo competirán entre ellos?

El soberano del espacio: reglas

Cuando penetramos en el mundo MMOG de *Second Life* como un personaje nuevo, recibimos una explicación sobre las reglas del juego. Algunas de estas reglas son las técnicas que necesitaremos para desplazarnos por *Second Life* —cómo movernos o cómo volar; otras son órdenes normativas que nos señalan lo que podemos hacer y lo que no.

Es imposible afrontar esta introducción sin darse cuenta de que estas restricciones provienen de una construcción humana. Dios no creó *Second Life*, y nadie sufre ninguna confusión al respecto. Tampoco es probable que quien penetre en este espacio pase por alto que una dimensión importante de dicha construcción se realiza mediante código. El hecho de que podamos volar es una decisión de los desarrolladores del código; también lo es adónde podemos volar; o el hecho de que se desplace una ventana de advertencia cuando chocamos con alguien; y también es una decisión de los desarrolladores del código que podamos desactivar las conversaciones de mensajería instantánea con aquéllos de los que no queremos saber nada. Nadie ignora que en *Second Life* se han tomado *decisiones*. Todo el mundo reconoce, pues, que una parte crucial del mundo del ciberespacio está construida mediante código. Tal y como me lo expresó el director ejecutivo de *Second Life*, Philip Roselade: «¿Qué representa Dios en un mundo virtual? Tu único Dios es el código».[1]

Ahora bien, como he afirmado desde el principio, deberíamos distinguir entre espacios muy controladores y escasamente controladores. Espacios como *Second Life* controlan ampliamente la vida de las personas que juegan en ellos. De hecho, el objetivo general del juego es crear la impresión de que uno está *allí*. Éstos, una vez más, son el tipo de lugares a los que denomino ciberespacio.

El ciberespacio es muy diferente a la vida en sitios web de pago de facturas o de correo electrónico. Éstos también están controlados por el código, pero en ellos el control, o la soberanía, es diferente que en *Second Life*. En este mundo virtual, o en lo que he definido en general como ciberespacio, el control es ubicuo; en un sitio web de pago de facturas, o en lo que he llamado Internet, el control es pasajero, transitorio.

Es interesante señalar que existe una importante dinámica de cambio que ya hemos identificado y que es más acusada en los espacios escasamente controladores. Se trata de la preferencia por controles basados en código allá donde éstos son posibles.

Pensemos de nuevo en el sitio web de pago de facturas. Por descontado, va contra la ley acceder a una cuenta bancaria ajena y transferir fondos sin la autorización de su titular. Ahora bien, ningún banco se limitaría jamás a fiarse de la ley para hacer cumplir esa norma, sino que todos ellos añaden un complejo conjunto de código para autentificar la identidad del usuario

---

1 Grabación de audio: entrevista con Philip Rosedale II (13 de enero de 2006; transcripción en el archivo con el nombre del autor).

cuando entra en un sitio web de pago de facturas. Allá donde pueda codificarse un objetivo de la política de una entidad, la única limitación de dicha codificación es la confrontación entre el coste marginal del código y el beneficio marginal del control añadido.

En cambio, en los entornos ampliamente controladores como *Second Life*, existe un límite en el uso del código para guiar la conducta social. En otras palabras, en ocasiones un código mejor puede debilitar la comunidad. Tal y como afirma el director ejecutivo de *Second Life*:

> En cierta forma, la dificultad de *Second Life* constituye un beneficio porque exige que te enseñen. Y el acto de ser enseñado es enormemente provechoso tanto para el profesor como para el estudiante [...] Hemos logrado que se produzca esta especie de tutelaje, que supone una relación muy estimulante psicológicamente —una que el mundo real no nos proporciona en demasía.[2]

Más importante aún resulta un segundo modo en que el código puede debilitar la comunidad. Tal y como es, *Second Life* no permite fácilmente la segregación entre la gente. Como describía Rosedale:

> En *Second Life* básicamente no hay zonificación alguna. Esto implica que las disputas vecinales son frecuentes. Ahora bien, desde el punto de vista del aprendizaje, éste es en realidad un aspecto positivo. He recibido correos electrónicos de gente que declara: «Bueno, yo no me llevaba bien con mis vecinos y, de resultas, aprendí muy rápido un montón de cosas acerca de cómo resolver nuestras disputas». [...] En el mundo real [...], hay tanta legislación [...] que en realidad no tienes que hablar con tus vecinos. En lugar de ello, simplemente hay una ley que dice que puedes o no puedes hacer algo. [...] En el mundo virtual, se da una oportunidad de comunicarse e interactuar que el mundo real sólo ofrece en circunstancias muy excepcionales.[3]

Por lo tanto, el código no hace desaparecer todos los problemas de un plumazo, no elimina la necesidad de que los vecinos solventen sus disputas y, así, contribuye a construir una comunidad. La práctica de la interacción crea lazos que no aparecerían si el código produjera los mismos resultados de forma automática. De esta forma, el diseño óptimo deja que sean los jugadores quienes resuelvan ciertos problemas —no porque la solución no pueda ser codificada, sino porque codificarla acarrearía costes colaterales.

---

2 *Ibidem*, pp. 4-6.

3 *Ibidem*, p. 5.

No obstante, sigue siendo el soberano de estos espacios virtuales quien elige una modalidad en lugar de otra. La compensación es complicada. La eficacia perfecta de los resultados no siempre es perfectamente eficaz, con lo que la elección de los medios sigue pendiente.

El soberano del espacio: elegir las reglas

Pero, ¿cómo se lleva a cabo esa elección? O más directamente, ¿qué hay de la democracia? En el espacio real, la regla es que los soberanos son legítimos sólo si son democráticos, de modo que apenas toleramos (la mayoría de) regímenes que no son democráticos. Así, la norma general para la vida del espacio real es que, en última instancia, el pueblo es soberano.

No obstante, el atraso singular que resulta más interesante en el ciberespacio es que, de nuevo, como lo expresa Castronova: «Uno no encuentra ni rastro de democracia en los mundos sintéticos».[4] La única excepción real es un mundo llamado *A Tale in the Desert*.[5] La democracia no se ha expandido a través del ciberespacio, o en Internet, sino que constituye más bien una rara excepción a una regla bastante sólida —que el «propietario» del espacio es el soberano. Y a juicio de Castronova, dicho propietario no suele ser un soberano demasiado bueno:

> En síntesis, ninguno de estos mundos ha desarrollado nunca, que yo sepa, instituciones de buen gobierno. En todos ellos reina la anarquía.[6]

Esto no equivale a afirmar que las opiniones colectivas no importen en el ciberespacio. De hecho, resultan cruciales para aspectos centrales de Internet tal y como es en este momento. Una suerte de votación —manifestada mediante los enlaces— guía los motores de búsqueda; Technorati, como ya he descrito, se basa en este mismo proceso para clasificar los *blogs*; y sitios web importantes, como Slashdot, emplean rutinariamente clasificaciones o votos de los editores para determinar qué comentarios saltarán a la primera plana.

---

4 Castronova, *Synthetic Worlds, op.cit.*, p. 207.

5 *Ibidem*, p. 216.

6 *Ibidem*, p. 213.

Todos estos sistemas se parecen a la democracia, pero no son democráticos. La democracia es la práctica por la que el pueblo elige las reglas que gobernarán un lugar determinado. Y, a excepción de la Wikipedia y *A Tale in the Desert*, son muy escasas las instituciones importantes de Internet o del ciberespacio donde impere la soberanía popular.

¿Cómo se explica este déficit democrático? ¿Deberíamos esperar que cambie?

Nuestra historia de autogobierno posee una forma específica, con dos rasgos en gran medida contingentes. Antes de la promulgación de la Constitución, la vida se basaba en la geografía —una nación era una sociedad situada en un espacio físico que guardaba lealtad a un único soberano. Tal y como consideraremos más extensamente en el próximo capítulo, la revolución conceptual de la república estadounidense consistió en que los ciudadanos podían tener dos soberanos —o, para ser más precisos, que ellos (en tanto que soberanos últimos) podían conferir su poder soberano a dos delegados diferentes. Un delegado era el gobierno de su Estado y el otro era el gobierno federal. De este modo, los individuos que vivían en un solo emplazamiento geográfico podían ser ciudadanos sometidos a ambos gobiernos. Tal era la idea recogida en el documento fundacional, como explicitó la Decimocuarta Enmienda: «Toda persona nacida o naturalizada en EEUU, y sometida a su jurisdicción, es ciudadana de EEUU y del Estado en que resida».

Este sentido de la ciudadanía no siempre comportaba el derecho a contribuir al autogobierno de la comunidad de la que se era ciudadano.[7] Aun hoy sigue habiendo ciudadanos sin derecho a voto —los niños, por ejemplo. Pero para aquéllos reconocidos como miembros de la sociedad civil y política, la ciudadanía supone el derecho a participar en el gobierno de la comunidad política de la que son miembros. Como ciudadano estadounidense, tengo derecho a votar en las elecciones de EEUU; como ciudadano californiano, tengo derecho a votar en las elecciones del Estado de California. Y tengo ambos derechos simultáneamente.

---

7 Véase Judith N. Shklar, *American Citizenship: The Quest for Inclusion*, Cambridge (Mass.), Harvard University Press, 1991, pp. 25–62; James A. Gardner, «Liberty, Community, and the Constitutional Structure of Political Influence: A Reconsideration of the Right to Vote», *University of Pennsylvania Law Review*, núm. 145, 1997, p. 893; Chandler Davidson y Bernard Grofman (eds.) *Quiet Revolution in the South,* Princeton (NJ), Princeton University Press, 1994, pp. 21–36.

A este nivel, el vínculo entre el derecho de ciudadanía y la geografía tiene todo su sentido. Ahora bien, a medida que se ha incrementado la movilidad, la obviedad que antaño caracterizó a tal vínculo se ha vuelto cada vez menos obvia. Yo vivo en San Francisco pero trabajo en Palo Alto. En mi caso, las leyes me reconocen plenos derechos de participación en San Francisco, pero ninguno en Palo Alto. ¿Por qué tiene sentido esto?

Hace tiempo que los teóricos políticos repararon en este problema.[8] Eruditos como Richard Ford o Lani Guinier han desarrollado pujantes concepciones alternativas del autogobierno que permitirían una variante de éste no directamente ligada a la geografía. Con una de ellas, los votantes eligen (dentro de unos límites) la comunidad donde influirán sus votos. Así, si yo estimara que participar en el futuro de Palo Alto es más importante que hacerlo en el futuro de San Francisco, tendría derecho a votar en Palo Alto aunque viviera en San Francisco.

Estas complicaciones en torno a la ciudadanía aumentan cuando consideramos el vínculo entre geografía y ciberespacio. Incluso si yo debiera tener derecho a votar en la comunidad donde trabajo, ¿debería tenerlo también en la comunidad donde juego? ¿Por qué los ciudadanos del espacio real necesitarían ejercer un control sobre los ciberlugares o sus arquitecturas? Puede que alguien pase la mayor parte de su vida en un centro comercial, pero nadie diría que eso le da derecho a controlar su arquitectura; o puede que a alguien le guste visitar Disney World todos los fines de semana, pero resultaría chocante que reivindicara por ello su derecho a regular Disney World. ¿Por qué el ciberespacio no se asemeja más a un centro comercial o un parque temático que al distrito donde vivimos y votamos?

Nuestra relación con un centro comercial o con Disney World no es más que una relación cliente-vendedor. Si a alguien no le gusta el Big Mac («dos rodajas de carne de vaca, salsa especial, lechuga, cebolla, pepinillo y queso en un pan recubierto de semillas de sésamo»), puede ir a Burger King; McDonald´s no está obligado a dejarle votar sobre el modo de preparar sus hamburguesas. Del mismo modo, si a alguien no le gusta el centro comercial local, puede ir a otro.

---

8 Véase Lani Guinier, *The Tyranny of the Majority: Fundamental Fairness in Representative Democracy*, Nueva York, Free Press, 1994; Richard Thompson Ford, «Beyond Borders: A Partial Response to Richard Briffault», *Stanford Law Review*, núm. 48, 1996, p. 1173; Richard Thompson Ford, «Geography and Sovereignty: Jurisdictional Formation and Racial Segregation», *Stanford Law Review*, núm. 49, 1997, p. 1365; Jerry Frug, «Decentering Decentralization», *University of Chicago Law Review*, núm. 60, 1993, p. 253; Jerry Frug, «The Geography of Community», *Stanford Law Review*, núm. 48, 1996, p. 1047.

El poder que el cliente tiene sobre estas instituciones es su capacidad para marcharse si no le gustan. Ellas compiten por su atención y su fidelización; si lo hacen bien, el cliente les será fiel; si no, se irá a otro sitio. Tal competencia resulta, pues, crucial para disciplinar a estas instituciones. Lo que las mueve a trabajar bien es esta competencia entre potenciales destinos de la clientela.

Esta parte de nuestra vida es importante. De hecho, es la parte en la que pasamos la mayor parte de nuestro tiempo, y la mayoría de la gente se encuentra más satisfecha con ella que con la parte en la que participa en las votaciones. En este sentido, todos estos lugares son soberanos, pues nos imponen sus reglas. Pero con respecto a los soberanos mercantiles, nos queda el recurso de marcharnos con la música a otra parte.

Con todo, la parte de nuestra vida regida por soberanos mercantiles no es la única; también hay parcelas de soberanía ciudadana. Así, no hay Estados que lleguen a decirles a sus ciudadanos: «No tiene usted derecho a votar aquí; si no le gusta, márchese». Nuestro papel en relación con nuestros Estados es el de una parte interesada que tiene voz: tenemos derecho —si tal Estado puede llamarse democrático— a participar en su estructuración.

Y esto no sólo es cierto en relación con nuestros Estados. Rara sería la universidad que no otorgara a su profesorado derecho a votar sobre asuntos centrales para ella (aunque no menos rara es la empresa que concede a sus empleados el derecho a votar sobre asuntos laborales); raro sería el club social que no otorgara a sus miembros cierto control sobre sus funciones —aunque, de nuevo, existen clubs que no lo hacen; incluso la Iglesia permite a sus miembros determinar en buena medida cómo se les va a gobernar. En estas instituciones somos miembros, no consumidores —o no sólo consumidores; y, en consecuencia, se nos otorga control sobre las reglas que nos gobernarán. En este sentido, en ellas impera la soberanía ciudadana.

En términos descriptivos, pues, el ciberespacio aún no está dominado (ni siquiera ampliamente poblado) por la soberanía ciudadana. Las soberanías que hemos visto hasta el momento son todas mercantiles, y esto es todavía más patente con respecto a Internet. En la medida en que los sitios web gozan de soberanía, ésta está en manos de soberanos mercantiles, y nuestra relación con ellos es la misma que tenemos con McDonald´s.

Ciertos teóricos han tratado de que estos dos modelos diferentes se fundan en uno solo: algunos han intentado trasladar el modelo de miembro a todas las esferas de la vida social —el lugar de trabajo, el centro comercial,

el bar—;[9] otros han hecho lo propio con el modelo de consumidor —los seguidores de Charles Tiebout, por ejemplo, han intentado explicar la competencia entre gobiernos de manera similar a como se explica nuestra elección entre pastas de dientes.[10] Pero aunque no podamos articular a la perfección las justificaciones para tratar estas elecciones de forma diferente, sería un error fundir estas distintas esferas en una sola. Sería un infierno tener que votar el diseño de nuestra pasta de dientes, y una tiranía que nuestro único recurso contra un Estado que no nos gustase fuera el exilio.

Pero entonces, ¿representa un problema que el ciberespacio se componga exclusivamente de soberanías comerciales? La primera defensa de dichas soberanías la desarrollan en sus escritos David Post y David Johnson, a veces de forma conjunta.[11] El artículo de Post «Anarchy, State, and the Internet» («Anarquía, Estado e Internet») es el que mejor compendia esta postura. Las comunidades del ciberespacio, sostiene Post, son gobernadas mediante «reglamentos», que podemos entender como los requisitos, integrados en la arquitectura o promulgados en un conjunto de reglas, que restringen la conducta en un lugar determinado. El mundo del ciberespacio, según él, se compone de este tipo de reglamentos, entre los cuales los individuos eligen cuál acatar. Puesto que estos reglamentos compiten por nuestra atención, el mundo del ciberespacio quedará definido por la competencia entre soberanos mercantiles para captar a su clientela.

---

9 Véase Michael Walzer, *Spheres of Justice: A Defense of Pluralism and Equality*, Nueva York, Basic Books, 1983 [ed. cast.: *Las esferas de la justicia: una defensa del pluralismo y la igualdad*, México, Fondo de Cultura Económica, 1997].

10 Véase Charles M. Tiebout, «A Pure Theory of Local Expenditures», *Journal of Political Economy*, núm. 64, 1956, p. 416; véase también Clayton P. Gillette, *Local Government Law: Cases and Materials*, Boston, Little Brown, 1994, p. 382; Vicki Been, «"Exit" as a Constraint on Land Use Exactions: Rethinking the Unconstitutional Conditions Doctrine», *Columbia Law Review*, núm. 91, 1991, pp. 473, 514-528.

11 Véase David G. Post, «Governing Cyberspace», *Wayne Law Review*, núm. 43, 1996, p. 155; David Post, «The New Electronic Federalism», *American Lawyer*, octubre de 1996, p. 93; David G. Post, «The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed», *Indiana Journal of Global Legal Studies*, núm. 5, 1998, pp. 521, 539; David R. Johnson y Kevin A. Marks, «Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?», *Villanova Law Review*, núm. 38, 1993, p. 487; Johnson y Post, «Law and Borders—The Rise of Law in Cyberspace», *Stanford Law Review*, núm. 48, 1996, pp. 1367-1375; David G. Post, «Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace», *Journal of Online Law*, 1995, artículo 3, disponible en http://www.wm.edu/law/publications/jol/articles/post.shtml.

La explicación de Post es de nuevo descriptivamente precisa; y también, defiende el autor, normativamente recomendada. Deberíamos entender a los soberanos tal y como se entiende el poder de mercado de una empresa en el marco de las leyes antimonopolio. Con el término «poder de mercado» los abogados especializados en regulación antimonopolio y los economistas se refieren a la capacidad de una empresa para aumentar los precios de manera rentable. En un mercado perfectamente competitivo, una empresa sin poder de mercado es aquélla que no puede aumentar sus precios porque caerían tanto sus ventas que no le compensaría dicho aumento.[12] La empresa que sí dispone de poder de mercado puede aumentar los precios y ver cómo se incrementan sus beneficios, amén de obligar a los consumidores a pagar por una mercancía un precio superior al de un mercado competitivo.

Podríamos imaginarnos una restricción análoga operando sobre los Estados. Los soberanos, como las empresas, pueden gozar de impunidad hasta un límite. A medida que se hacen más represivos, o que regulan con mayor severidad, otros soberanos, u otros reglamentos, se convierten en sus competidores. Llegados a cierto punto, para los ciudadanos es más fácil marcharse que soportar las cargas de la regulación,[13] es más fácil eludir la ley que cumplirla.

Dado que tales desplazamientos son costosos en el espacio real, los soberanos pueden, al menos a corto plazo, salirse habitualmente con la suya. En el ciberespacio, sin embargo, los desplazamientos no son tan complicados. Si no nos gusta el reglamento del MMOG al que jugamos, podemos pasarnos a otro; si no nos gusta la cantidad de publicidad que hay en un portal de Internet, en dos segundos podemos cambiar nuestra página de inicio. La vida en el ciberespacio consiste en agregarse a grupos sin ni siquiera moverse de casa. Si el grupo al que nos agregamos no nos trata como queremos, podemos abandonarlo. Puesto que la presión competitiva es mayor en el ciberespacio, los Estados y demás propagadores de reglamentos han de comportarse como empresas en un mercado competitivo.

Se trata de una concepción de la gobernanza importante e interesante: importante porque describe el gobierno en el ciberespacio, e interesante porque quizá pone de manifiesto el propósito y los límites de la soberanía ciudadana en el espacio real. Tal concepción argumenta a favor de un mundo de voluntarios donde las reglas no se impongan, sino que se seleccionen;

---

12 Véase Phillip E. Areeda *et al.*, *Antitrust Law,* vol. 2A, Boston, Little Brown, 1995, pp. 85-87.

13 Véase Post, «Anarchy, State, and the Internet», *op. cit.*, pp. 29-30.

un mundo que minimice los abusos de poder de cualquier Estado, convirtiéndolos en competidores por los ciudadanos. Se trata de una forma de gobierno estilo McDonald´s o Coca-Cola —ansiosa por complacer, temerosa de las revueltas.

Sin embargo, hay razones para el escepticismo respecto a esta postura. En primer lugar, reflexionemos acerca de la afirmación de que los costes de marcharse son menores en el ciberespacio que en el espacio real. Cuando cambiamos de proveedor de servicios de Internet o de portal, nos enfrentamos sin duda a un conjunto de «reglas» diferente, y estas reglas sin duda compiten por nuestra atención. Es exactamente como ir de un restaurante o de un centro comercial a otro. Existen reglamentos que compiten entre sí, los cuales constituyen uno de los diversos factores que tenemos en cuenta a la hora de elegir un proveedor de servicios de Internet; y en la medida en que hay una movilidad fácil entre estos reglamentos, este cambio de proveedor supone sin duda una competencia entre ellos. Algunos proveedores, por supuesto, tratan de dificultar este cambio. Si hemos sido miembros de AOL durante diez años y decidimos pasarnos a otra compañía, AOL no nos facilitará las cosas, poniendo trabas, por ejemplo, a que transfiramos a la nueva cuenta nuestros correos electrónicos. No obstante, cuando la gente reconozca esta restricción impuesta por AOL, elegirá otro proveedor de servicios de Internet. Si la competencia es real, los reglamentos competirán entre sí.

Las comunidades, sin embargo, funcionan de otra forma. Consideremos, por ejemplo, la «competencia» entre distintos MMOG. La gente se suscribe a ellos y pasa meses construyendo su propio personaje, además de acumulando activos —edificios que ha construido o armas que ha adquirido. Ambos recursos constituyen una especie de capital: la trama de relaciones desarrolladas es el capital social y todas las cosas acumuladas, el capital físico.

Por ende, si nos sentimos insatisfechos con la vida en el MMOG que hemos elegido, podemos marcharnos de él, pero hacerlo nos saldrá caro: no podemos transferir el capital social que hemos construido y, dependiendo del juego, puede que tampoco podamos transferir el capital físico. Al igual que la opción de cambiarse a otro programa de fidelización de viajeros, la opción de suscribirse a otro MMOG es una decisión que implica desperdiciar ciertos activos. Y tal condicionante debilitará la competencia entre estos reglamentos.

No pretendo exagerar este argumento. De hecho, debido al desarrollo de mercados de venta de activos dentro de los MMOG y a la estandarización de la naturaleza de los juegos, algunos defienden que cada vez resulta más

sencillo trasladarse de un juego a otro. En el espacio real tampoco se puede transferir fácilmente el capital social de una comunidad a otra. Los amigos no son bienes fungibles, por más que puedan proporcionarnos contactos en nuestro nuevo lugar de residencia. Los activos físicos, sin embargo, sí son transferibles en el espacio real, donde puedo vender aquello que no quiero y llevar conmigo lo que deseo conservar. En los MMOG esto no siempre es posible; en el espacio real, sí.

Paradójicamente, pues, podríamos afirmar que cambiar de comunidad puede ser más complicado en el ciberespacio que en el espacio real. Y ello porque al pasar de una cibercomunidad a otra, hemos de renunciar a todas nuestras pertenencias, mientras que en el espacio real podemos llevar muchas de ellas con nosotros.[14] Las comunidades del ciberespacio pueden, a corto plazo, disponer de más poder sobre sus ciudadanos (por lo que respecta al capital social) que las comunidades del espacio real.

Lo expuesto hasta aquí supone que el panorama de la competencia de reglamentos en el ciberespacio es más complejo de lo que sugiere David Post, si bien la presión competitiva es a su vez potencialmente mayor. Esto podría provocar en las comunidades del ciberespacio un deseo de evolucionar hacia la soberanía ciudadana, si bien de nuevo hay que reconocer que aún no abundan las pruebas de tal evolución.

Existe una segunda razón más fundamental para el escepticismo. Aunque pudiéramos construir el ciberespacio según el modelo del mercado —de modo que nos relacionáramos con los espacios del ciberespacio de la misma forma que lo hacemos con la pasta de dientes en el espacio real—, tenemos razones de peso para no hacerlo. A medida que la vida se traslada a la Red, y que cada vez más ciudadanos de los estados X, Y y Z acuden a interactuar a los ciberespacios A, B y C, éstos pueden necesitar desarrollar la clase de responsabilidad y atención que se desarrolla (idealmente) en el seno de una democracia. O dicho de otro modo, si el ciberespacio quiere que se le reconozca su propia soberanía legítima, y así merecer cierto grado de independencia y respeto, debe transformarse más claramente en un espacio de soberanía ciudadana.

---

14 En el tiempo transcurrido desde la primera versión de *El código*, este argumento se ha vuelto mucho más cuestionable. La capacidad efectiva de los jugadores de pasar de un juego a otro ha aumentado. Se trata de otra muestra de que el espacio real y el ciberespacio se asemejan cada vez más.

Esta misma dinámica se da en el espacio real. Hay muchas instituciones que no son «soberanas» en el sentido de que controlen cómo vive la gente, sino en el sentido de que controlan cómo se comporta la gente en el seno de dicha institución. Las universidades, los clubs sociales, las Iglesias y las empresas constituyen ejemplos obvios de instituciones que adquieren cierto grado de autonomía con respecto al gobierno ordinario. Tal autonomía puede ser amplia o reducida, y lo que sugiero aquí es que será más amplia cuanto más refleje la institución los principios de la soberanía ciudadana.

Esta clase de soberanía se expresa legalmente por medio de doctrinas de inmunidad. Una empresa goza de ciertas exenciones pero ello depende de que se ajuste a una forma empresarial concreta; lo mismo sucede con las Iglesias, si bien a medida que su forma de gobierno se hace más abstrusa, su inmunidad se cuestiona cada vez más.

Las comunidades del ciberespacio adquirirán más rápido una inmunidad similar si reflejan los principios de la soberanía ciudadana que si reflejan los de la soberanía mercantil. Cuanto más responsables se vuelvan dichas comunidades, más probable es que los Estados del espacio real admitan sus normas por medio de doctrinas como la de la inmunidad.

Es obvio que esta maduración —si es eso lo que es— tiene aún por delante un largo camino. Tal evolución depende de que los miembros de estas comunidades del ciberespacio reconozcan progresivamente que éstas son, en cierto sentido, independientes o complementarias; y también depende de que quienes no sean miembros de ellas reconozcan que hay algo distintivo en estas comunidades. Algunos se muestran optimistas al respecto, y así Dan Hunter y Greg Lastowka escriben:

> Los tribunales tendrán que reconocer que los mundos virtuales constituyen jurisdicciones separadas de nuestro mundo, con sus propios derechos, normas y leyes distintivas. Aunque los habitantes cibernéticos demandarán el reconocimiento de estos derechos por parte de los tribunales del mundo real y los administradores del mundo virtual, necesitarán alcanzar tales derechos por sí mismos en el contexto de los mundos virtuales.[15]

Algo similar a esta progresión lo hemos visto en nuestra propia historia. Hubo una época en la que Estados Unidos era realmente «los Estados unidos», una época en la que la realidad política dominante era local y existían

15 Gregory Lastowka y Dan Hunter, «The Laws of Virtual Worlds», *California Law Review*, núm. 92, 2004, pp. 1-73.

verdaderas diferencias de cultura y de valores entre el Estado de Nueva York y el de Virginia. Pese a estas diferencias, en 1789, estos Estados se unieron para establecer un Estado nacional relativamente reducido. Tal Estado había de ser mínimo y limitado, con una serie de propósitos acotados y estrictamente articulados que no debía rebasar.

Estos límites tenían sentido en la limitada comunidad que era por entonces EEUU, donde los diferentes Estados poseían muy pocos rasgos compartidos como nación. Tenían en común una historia de victoria sobre el ejército más poderoso del mundo y un propósito de expandirse por un continente casi infinito,[16] pero no compartían una vida social o política. La vida estadounidense se circunscribía a lo local, con intercambios relativamente infrecuentes, y en un mundo así tenía sentido un Estado nacional de carácter limitado.

No obstante, había algunas cuestiones nacionales pendientes de articular y resolver. La esclavitud, por ejemplo, constituía un estigma para todo el país, por más que esta práctica se limitara a unos pocos Estados. En el proceso de fundación de EEUU se había debatido sobre la idoneidad de dejar la esclavitud en manos de la regulación local, pero la Constitución se basó en un acuerdo de transigencia en torno a esta cuestión. En consecuencia, no se permitió al Congreso abordar la cuestión de la «importación» de esclavos hasta 1808.[17] A partir de entonces tuvo la posibilidad, y cada vez más estadounidenses reclamaron que debía hacerlo. Sin embargo, la esclavitud continuó siendo una lacra en la reputación moral de nuestra nación, pues aunque el Congreso pudo eliminarla al menos en los Estados del norte, se defendía que debía hacerlo también en los Estados sureños.

Quienes se oponían a esta reivindicación de que el Congreso purgara nuestra nación de la esclavitud se clasificaban en dos categorías. Una era la de aquéllos que apoyaban la institución de la esclavitud y estaban convencidos de que era fundamental en la vida sureña; la otra, que es la que verdaderamente me

---

16 Al menos tres de las cuatro regiones originarias de EEUU comparten esta historia; véase Fischer, *Albion's Seed*, *op. cit.*, *pp.* 827-828.

17 El Artículo V de la Constitución declara (de manera críptica, sin duda) que «ninguna Enmienda que pueda redactarse antes del año mil ochocientos ocho puede afectar de ninguna manera a las Cláusulas primera y cuarta de la Sección Novena del Artículo primero». Dichas Cláusulas declaran lo siguiente: «(1) El Congreso no prohibirá antes del año mil ochocientos ocho la migración o importación de tales personas que cualquiera de los Estados ahora existentes estime oportuno admitir, pero puede imponer sobre dicha importación un impuesto o contribución que no exceda los diez dólares por persona»; y (4) «No se establecerá ningún impuesto de capitación, ni ningún otro impuesto directo, como no sea proporcionalmente al censo o recuento que se ordenó realizar anteriormente».

interesa aquí, era la de aquéllos que, con perfecto candor e integridad, sostenían que la esclavitud era un asunto local, no nacional, que así lo habían interpretado los padres de la Constitución y que, por lo tanto, el Estado nacional debería desentenderse de ella.

Por muy cierta que esta afirmación pudiera haber sido en 1791 o en 1828, con el paso del tiempo se volvió menos convincente. A medida que la nación se integraba social y económicamente cada vez más, la verosimilitud de afirmar «Yo, ante todo, soy de Virginia» disminuía, al tiempo que aumentaba la importancia de ser ciudadano de la nación en su conjunto.[18]

Este cambio no sobrevino a través de decisiones políticas sino como resultado de una realidad económica y social cambiante. Nuestro sentido de pertenencia a una comunidad nacional creció hasta tal punto que se hizo imposible negar nuestra ciudadanía nacional. Una guerra produjo este reconocimiento, la Decimocuarta Enmienda lo plasmó por escrito en la Constitución y los intercambios económicos y sociales lo dotaron de plena realidad. Y a medida que tal cambio se consolidaba, las reivindicaciones de que cuestiones como la esclavitud se ceñían al ámbito local se volvieron absurdas.

En la actualidad estamos viviendo exactamente el mismo proceso, a escala internacional, y el ciberespacio está contribuyendo a él de forma importante. Tal proceso, por supuesto, venía adquiriendo velocidad desde el final de la Segunda Guerra Mundial, pero Internet lo ha acelerado frenéticamente. Los ciudadanos de a pie se hallan conectados al resto del mundo y pueden efectuar transacciones internacionales sin precedentes. La presencia de una comunidad que está más allá de cualquier Estado particular resulta cada vez más innegable.

A medida que esta comunidad se desarrolle en el ciberespacio, sus ciudadanos tendrán cada vez más difícil permanecer neutrales en este espacio internacional. Del mismo modo que en 1791 un ciudadano de principios podría haber afirmado que la esclavitud en el Estado de Virginia era irrelevante para un ciudadano del Estado de Maine, puede que en 1991 el control de la libertad de expresión en Singapur fuera irrelevante para un ciudadano estadounidense. Ahora bien, igual que la reivindicación sobre la relevancia local de la esclavitud se hizo inverosímil en el transcurso del siglo XIX, la

---

18 Véase John F. Kennedy, *Profiles in Courage*, Nueva York, Harper, 1956, cap. 3 [ed. cast.: *Perfiles de Coraje*, trad por. Francisco Bermeosolo, Buenos Aires, Plaza & Janes, 1964].

reivindicación con respecto a la libertad de expresión en la red se convertirá en inverosímil en el siglo XXI. El ciberespacio es una comunidad internacional que ha de dar respuesta a interrogantes constitucionales ante los que no cabe apartarse simplemente del espacio internacional alegando que se trata de cuestiones locales.

Al menos no cabría decir eso una vez que en 1995 invadimos efectivamente dicho espacio internacional por medio de Internet. Ese año lanzamos al mundo una arquitectura que facilitaba extraordinariamente la libertad de expresión y la privacidad, posibilitando comunicaciones seguras mediante un protocolo que permitía el cifrado y alentando comunicaciones libres mediante un protocolo resistente a la censura. He aquí la arquitectura de expresión que la red aportó al mundo —que los estadounidenses aportamos al mundo.

Ahora estamos modificando esa arquitectura: estamos permitiendo el comercio como nunca antes hicimos, estamos contemplando la posibilidad de regular el cifrado, estamos facilitando el control de la identidad y de los contenidos. En definitiva, estamos reconstruyendo los principios de la Red, ante lo cual la pregunta es: ¿podemos comprometernos con la neutralidad en esta reconstrucción de la arquitectura de la Red?

No creo que podamos; ni que debamos; ni que vayamos a hacerlo. Así como los estadounidenses de 1861 no pudieron permanecer neutrales ante la cuestión de la esclavitud, nosotros tampoco podemos hacerlo ante la cuestión de si la red debería posibilitar un control centralizado de la expresión. Deberíamos comprender que estamos inmersos en una batalla política de alcance mundial; que poseemos nociones acerca de los derechos que deberían garantizarse a todo ser humano, independientemente de su nacionalidad; y que deberíamos estar preparados para impulsar dichas nociones en este nuevo espacio político abierto por la red.

No estoy haciendo un alegato a favor de un Estado mundial; de hecho, la imposibilidad de tal idea constituye el eje de buena parte del próximo capítulo. Lo que defiendo más bien es que debemos responsabilizarnos del componente político que integramos en esta arquitectura, pues dicha arquitectura es un soberano que gobierna la comunidad residente en ese espacio. En definitiva, debemos reflexionar sobre la dimensión política de las arquitecturas de la vida en la Red.

He afirmado que deberíamos considerar el código en el ciberespacio como su propio régimen de regulación, y que este código en ocasiones puede entrar en competencia con el régimen regulador de la ley. Por ejemplo,

hemos visto cómo la ley de copyright podía ser incoherente con el régimen de regulación de los sistemas de confianza. Lo que defiendo es que deberíamos entender que estos dos regímenes reguladores compiten entre sí. Necesitamos, por lo tanto, un modo de elegir entre ellos, de decidir cuál debería prevalecer.

A medida que este sistema de regulación por medio de código se desarrolle, contendrá sus propias normas y las expresará en sus estructuras o en las reglas que imponga. Si los pronósticos legales y económicos son correctos, estas normas serán sin duda eficaces, y puede que también sean justas; pero en la medida en que la justicia no le siga la pista a la eficacia, dichas normas serán eficaces pero injustas. La cuestión será entonces: ¿cómo reaccionamos ante esta brecha?

En esta competencia entre código y ley se da una pauta importante. La ley, al menos tal como regula las relaciones internacionales, es el fruto de negociaciones dilatadas. Los países deben llegar a un acuerdo sobre el modo en que la ley regulará y sobre cualquier norma que impongan al ordenamiento privado. A medida que su tarea se relaciona con el ciberespacio en concreto, estos acuerdos revisten una especial importancia. Alcanzarlos requerirá que las naciones del mundo lleguen a una comprensión común acerca de este espacio y desarrollen una estrategia común para abordar su regulación.

15. Competencia entre soberanos

Conflictos

Presento a continuación dos historias acerca del poder de la soberanía, una que probablemente le suene al lector, y otra que no.

1. Protegiendo a los franceses

A los franceses no les gustan los nazis (reprímase el impulso francófobo de añadir «ya no» a la frase; recordemos que si no fuera por los franceses, es probable que los estadounidenses no tuviéramos una nación). La ley francesa no permite que los nazis contraataquen y así, al igual que en Alemania, en Francia se estipula como delito promover el Partido Nazi o vender su parafernalia. Los franceses vigilan que este virus ideológico no renazca en Europa.

La ley francesa es distinta de la estadounidense en este aspecto. La Primera Enmienda bloquearía cualquier limitación de la propaganda política basada en la opinión. El Estado no está más habilitado para bloquear la venta de parafernalia nazi de lo que lo está para bloquear la venta de chapas del Partido Republicano. La libertad de expresión implica que la opinión de que algo es una reliquia política no puede determinar si esa reliquia puede o no venderse.

Yahoo! es una empresa estadounidense que en 1999 abrió una sucursal francesa, Yahoo! Francia, donde habilitó un sitio de subastas.[1] Al igual que eBay, este sitio permitía que sus usuarios elaboraran una lista de objetos a subastar; e igual que eBay, este sitio organizaba la subasta y contribuía a facilitar la venta final de los objetos subastados.

Poco después de que abriera, y contraviniendo la legislación francesa, comenzó a aparecer parafernalia nazi en el sitio de subastas de Yahoo! Francia. Hubo gente en Francia a la que esto no le hizo ninguna gracia, y en el año 2000 se interpuso una demanda contra Yahoo! instándole a que retirara la parafernalia nazi de su sitio o bloqueara el acceso a ella.[2]

Esto a su vez no le hizo ninguna gracia a Yahoo!, que insistía en que se trataba de Internet, un medio global en el que no hay modo de bloquear a los franceses el acceso a los sitios de Yahoo! Además sería absurdo que las reglas de un país se convirtieran en las reglas de todo el mundo. Si cada uno de los países pudiera obligar a todos los sitios web del mundo a acatar sus propias leyes, se produciría una carrera de homologación a la baja (o al alza, dependiendo de la perspectiva de cada cual), por lo que Francia debería limitarse a aceptar que en el mundo de Internet su dominio no es absoluto. El Noveno Circuito de Apelaciones resumió así el argumento de Yahoo!: «Yahoo! desea una decisión que proporcione la amplia protección de la Primera Enmienda a la expresión [...] en Internet que pudiera violar las leyes [...] de otros países».[3]

El juez francés, Jean Jacques Gómez, no estaba de acuerdo con Yahoo!, y en la sentencia que dictó en mayo de 2000 exigió a la empresa que retirara la parafernalia nazi de su sitio o bloquease el acceso a los ciudadanos franceses.[4] En un segundo fallo dictado en noviembre del mismo año, el tribunal francés instó a Yahoo! a cumplir la sentencia en el plazo de tres meses, o a pagar cien mil francos por cada día de demora.[5]

---

1 La historia del pleito se cuenta en *Yahoo! Inc. vs. La Ligue Contre le Racisme*, 433 F. 3º, 1199, 9º Cir., 2006. Véase también Jack Goldsmith y Timothy Wu, *Who Controls the Internet: Illusions of a Borderless World*, *op. cit.*; Michael Geist, «Is There a There There? Towards Greater Certainty for Internet Jurisdiction», *Berkeley Technology Law Journal*, núm. 16, 2001, p. 1345. Para una crítica del conflicto (y de su relevancia) véase Marc H. Greenberg, «A Return to Lilliput: The LICRA vs. Yahoo! Case and the Regulation of Online Content in the World Market», *Berkeley Technology Law Journal*, núm. 18, 2003, p. 1191.

2 *Yahoo! Inc. vs. La Ligue Contre le Racisme*, 433 F. 3º, 1199, 9º Cir., 2006.

3 *Ibidem*, p. 1223.

4 Véase «France Bans Internet Nazi Auctions», BBC NEWS, 23 de mayo de 2000, disponible en http://news.bbc.co.uk/1/hi/world/europe/760782.stm.

5 *Yahoo! Inc. vs. La Ligue Contre le Racisme*, 433 F. 3º, 1199, 9º Cir., 2006.

La Red estaba indignada. Miles de sitios web criticaron la sentencia del tribunal francés y cientos de periódicos siguieron el juicio. Francia estaba destruyendo la «libertad de expresión» en Internet al imponer sus normas a cualquiera que usara Internet desde cualquier lugar. Como comentó Adam Thierer, del Cato Institute:

> Afortunadamente los estadounidenses se toman la libertad de expresión un poco más en serio que los británicos, los franceses, los alemanes y el resto del mundo. Y sí, EEUU podría convertirse en el guardián de la libertad de expresión a escala mundial al ofrecer en la Red la protección de la Primera Enmienda a millones de personas cuyo derecho a expresarse libremente se ve coartado en sus propios países.[6]

2. Protegiendo a Hollywood

En el 2000 un empresario televisivo llamado Bill Craig lanzó iCraveTV, un servicio de televisión radicado en Toronto que se diseñó para emitir la programación televisiva ordinaria a través de las líneas de Internet. De acuerdo con la legislación canadiense, o al menos con la interpretación de aquel momento,[7] iCraveTV estaba convencida de que no necesitaba permiso para ello. En efecto, la ley de Canadá permitía usar cualquier tecnología para extender el alcance de una emisión, siempre que dicha emisión no fuese alterada.[8] De este modo, Craig compró sus servidores, puso en marcha el flujo de emisiones y se sentó a esperar a que llegaran los espectadores. Y éstos llegaron, y lo hicieron a millones, con lo que iCraveTV se convirtió en un éxito instantáneo. Parecía que mucha más gente que el propio Craig se moría por la televisión.[9]

---

6 Adam D. Thierer, «Web Restrictions Unlikely to Muzzle Neo-Nazi Speech», Cato Institute Web Site, 15 de enero de 2001, disponible en http://www.cato.org/pub_display.php?pub_id=4400.

7 Disponible en http://news.cnet.com/Canada-blocks-free-Net-TV/2100-1023_3-981254.html?tag=st.ref.goo. John Borland, «Broadcasters Win Battle Against iCraveTV.com», *CNET NEWS*, 28 de enero de 2000, disponible en http://news.cnet.com/2100-1033-236255.html.

8 Michael Geist, «Is There a There There? Towards Greater Certainty for Internet Jurisdiction», *Berkeley Technology Law Journal*, núm. 16, 2001, p. 1345.

9 El autor realiza aquí un juego de palabras intraducible con el nombre con que Bill Craig bautizó su proyecto, iCraveTV (en inglés, «muero por la televisión»). [N. del E.]

Poco después del lanzamiento del proyecto, sin embargo, Craig empezó a descubrir que no a todo el mundo le había agradado su idea. En concreto, los titulares de copyright de EEUU no se mostraron entusiasmados con la televisión gratuita que había creado Craig. Y es que mientras que en Canadá uno era libre de retransmitir programas de televisión a través de Internet, en EEUU tal libertad no existía. La legislación estadounidense de copyright regula estrictamente el derecho a la retransmisión, y Craig la había incumplido.

iCraveTV adoptó algunas medidas para excluir a los residentes de EEUU, pero nadie podría realmente haber esperado que surtieran efecto. Al principio, iCraveTV se limitó a advertir a la gente de que sólo los canadienses podían usar el sitio. Más tarde iCraveTV añadió a su sitio un sistema de bloqueo basado en los prefijos —el usuario tenía que especificar su prefijo para acceder al sitio; si éste no correspondía al territorio de Canadá, se le denegaba el acceso—, pero no es difícil encontrar un prefijo canadiense (por ejemplo, el propio número de teléfono de iCraveTV aparecía destacado en su página web).

En cualquier caso, Craig no creía que fuera tarea suya vigilar las conductas infractoras de los estadounidenses. En Canadá emitir televisión a través de Internet no violaba ninguna ley, así que ¿por qué tenía que preocuparse de si lo hacía en EEUU?

Una partida de abogados estadounidenses convenció rápidamente a Craig de que tenía que preocuparse. En una demanda interpuesta en Pittsburgh, la NFL (*National Football League*, Liga Nacional de Fútbol Americano), junto con otras partes, acusaron a iCraveTV de infracción del copyright en EEUU. Fuera o no legal emitir televisión a través de Internet en Canadá, en EEUU no lo era. Por lo tanto, en la medida que los estadounidenses podían acceder a este sitio web canadiense, estaban violando la legislación de EEUU; y en la medida que dicho sitio web posibilitaba que los estadounidenses accedieran a él, estaba violando la legislación de EEUU. Así pues, la NFL solicitó al tribunal de Pittsburgh la clausura de este servidor canadiense.

El juez del Tribunal de Distrito de EEUU, Donald Ziegler, instruyó unas exhaustivas diligencias de determinación de hechos. El 8 de febrero del 2000 dicho tribunal emitió un requerimiento judicial por el que clausuraba iCraveTV y le concedía noventa días para demostrar que disponía de la tecnología necesaria para bloquear el acceso a los residentes de EEUU. iCraveTV prometió que, empleando algunas de las tecnologías de localización IP descritas en el Capítulo 4, podría bloquear el acceso al 98 % de ciudadanos estadounidenses. Pero tal porcentaje no era lo bastante bueno para el tribunal: si algún estadounidense podía acceder al sitio de iCraveTV, ésta estaba violando la legislación de EEUU.

iCraveTV no podía prometer un 100 % de efectividad en su bloqueo. A diferencia de lo ocurrido con la sentencia del juez Gómez en el caso de Francia, esta decisión judicial no provocó indignación alguna en la red. No hubo miles de sitios web que la criticaran, ni tan siquiera un puñado de editoriales cuestionándola; de hecho, casi nadie se percató de ella.

Ceguera recíproca

Los casos de Yahoo! Francia y de iCraveTV suscitaban la misma cuestión fundamental. En ambos se da una conducta que es legal en un país (vender parafernalia nazi en EEUU, emitir libremente televisión a través de Internet en Canadá), e ilegal en otro (vender parafernalia nazi en Francia, emitir gratuitamente televisión a través de Internet en EEUU). Y en ambos el juez del país cuyas leyes se estaban violando ejerció su poder para detener dicha violación (el juez Gomez ordenando a Yahoo! retirar el material nazi o bloquear su acceso desde Francia; el juez Ziegler ordenando a iCraveTV eliminar las emisiones televisivas de su sitio o bloquearlas para los estadounidenses). Sin embargo, en un caso se vilipendió este resultado calificándolo de «censura», mientras que en el otro pasó prácticamente desapercibido.

He aquí la ceguera recíproca. Vemos en los demás un defecto que no somos capaces de detectar en nosotros mismos. Para un estadounidense el bloqueo de la expresión de los nazis supone «censura», y sería el colmo demandar que tal expresión se censurara en EEUU —donde es legal— tan sólo porque es ilegal en Francia.

Pero ¿por qué no es «censura» bloquear la televisión gratuita en Canadá tan sólo porque sea ilegal en EEUU? En ambos casos, una expresión legal en un país es bloqueada en ese mismo país por un tribunal extranjero. EEUU impide a los canadienses disfrutar de retransmisiones televisivas gratuitas tan sólo porque éstas son ilegales en EEUU. Los franceses impiden a los estadounidenses adquirir parafernalia nazi en el sitio de subastas de Yahoo! tan sólo porque dicho material es ilegal en Francia.

Es más, en un aspecto importante, el caso de iCraveTV es peor que el de Yahoo! Y es que, en este último, el tribunal tuvo en cuenta las pruebas relativas a la capacidad de Yahoo! para adoptar medidas técnicas con las que

bloquear a los ciudadanos franceses.[10] Como enfatiza Joel Reidenberg,[11] el tribunal atribuyó a Yahoo! responsabilidad jurídica porque concluyó que existían medios técnicos razonables para bloquear el acceso al material nazi a los ciudadanos franceses. Esos medios no eran perfectos, pero el tribunal estimó que podría identificarse a más del 90 % de los usuarios franceses.[12] Pero en el caso de iCraveTV, aunque los medios técnicos aseguraban un 98 % de efectividad, el tribunal los desestimó por insuficientes. Por lo tanto, la restricción del tribunal estadounidense fue mayor que la del tribunal francés.

Los estadounidenses no poseen el monopolio de la ceguera; y mi propósito al seleccionar este caso no es meterme con ellos. Más bien creo que estos dos casos nos ofrecen una lección general. No habrá ninguna nación que no tenga algún tipo de expresión que quiera regular en Internet; todas ellas tienen algo que desean controlar. Ese algo, no obstante, diferirá de una nación a otra. Los franceses querrán regular la expresión nazi; los estadounidenses, la pornografía; los alemanes, ambas; los suecos, ninguna de ellas.

Este capítulo trata sobre estos deseos de control que se solapan. ¿Cómo conjugará Internet esta combinación? ¿De qué nación serán las leyes que se apliquen? ¿Hay alguna forma de evitar tanto la anarquía como la regulación total? ¿Determinarán los regímenes más restrictivos la libertad disponible para el resto de nosotros?

En mi opinión, hemos visto ya suficiente para saber cómo se desarrollará la historia. En lo que queda de capítulo describo dicho desarrollo, pero primero deberíamos dejar claro por qué se dará esta regulación del ciberespacio. Todos nosotros deberíamos reconocer el interés que el Estado tiene al respecto y cuán fuerte, o débil, es dicho interés. Y lo que es más importante, deberíamos reconocer cómo ha cambiado la arquitectura de la red para posibilitar la satisfacción de tal interés. Como escriben Jack Goldsith y Tim Wu:

---

10 *Yahoo! Inc. vs. La Ligue Contre le Racisme,* 433 F. 3º, 1199, 9º Cir., 2006.

11 Reidenberg señala que la traducción del fallo francés proporcionada al Tribunal del Distrito en EEUU era defectuosa. Joel R. Reidenberg, «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, núm. 153, 2005, pp. 1951, 1959.

12 *Yahoo! Inc. vs. La Ligue Contre le Racisme,* 433 F. 3º, 1199, 9º Cir., 2006.

> Los argumentos de Yahoo! tomaban como premisa la visión de los noventa de una Internet sin fronteras. Cinco años después, tal visión está siendo rápidamente reemplazada por la realidad de una Internet que se desintegra y refleja las fronteras nacionales. Lejos de allanar el mundo, Internet está conformándose de muchas maneras a las condiciones locales.[13]

Acerca de estar «en» el ciberespacio

El ciberespacio es un lugar.[14] La gente vive en él, y allí experimenta todo lo que experimenta en el espacio real, algunos incluso más. Esta experiencia, además, no se da como individuos aislados inmersos en un sofisticado juego de ordenador, sino como parte de grupos, en comunidades, entre desconocidos y entre personas a las que se llega a conocer y, a veces, a apreciar —o a amar.

Mientras están en ese lugar, el ciberespacio, también están aquí: frente al monitor, comiendo patatas fritas, ignorando el teléfono; en el ordenador de la planta de abajo mientras sus maridos duermen; en el trabajo, en los cibercafés y en los laboratorios informáticos. Viven esta vida en el ciberespacio mientras están aquí, y en algún momento del día se desconectan y entonces se encuentran sólo aquí. Se levantan del ordenador ligeramente aturdidos y se dan la vuelta. Ya han regresado.

Pero ¿dónde están cuando están en el ciberespacio?

Tenemos este deseo de elegir: queremos determinar si están en el ciberespacio o en el espacio real. Tenemos este deseo porque queremos saber a qué espacio corresponde la responsabilidad. ¿Qué espacio tiene jurisdicción sobre ellos? ¿Qué espacio manda?

---

13 Jack Goldsmith y Timothy Wu, *Who Controls the Internet: Illusions of a Borderless World*, *op. cit.*, 2006, p. 41.

14 Ha existido un debate rico, y en ocasiones innecesario, sobre si el ciberespacio constituye de hecho un «lugar». Sigo creyendo que el término es útil, y Dan Hunter confirma mi idea al menos parcialmente en Dan Hunter, «Cyberspace as Place and the Tragedy of the Digital Anticommons», *California Law Review*, núm. 91, 2003, p. 439. Michael Madison añade un argumento valioso acerca de aquello de lo que no da cuenta la metáfora del lugar en Michael J. Madison, «Rights of Access and the Shape of the Internet», *Boston College Law Review*, núm. 44, 2003, p. 433. Lemley también aporta una perspectiva importante; véase «Place and Cyberspace», *California Law Review*, núm. 91, 2003, p. 521.

La respuesta es ambos. Siempre que alguien está en el ciberespacio, también está aquí, en el espacio real. Siempre que alguien está sujeto a las normas de una comunidad del ciberespacio, también está viviendo en el seno de una comunidad del espacio real. Si estamos allí, entonces estamos en los dos lugares a la vez y se nos aplicarán las normas de ambos. El problema que tiene la ley es el de resolver cómo han de aplicarse las normas de ambas comunidades, dado que el sujeto a quien se le aplican puede estar en ambos lugares a la vez.

Retomemos el ejemplo de Jake Baker. El problema que había con él no era que fuese a un lugar diferente donde las normas también lo eran, sino que estaba simultáneamente en la habitación de una residencia de estudiantes de Michigan y en la Red. Estaba sujeto a las normas de urbanidad en la residencia y a las normas de indecencia en el ciberespacio; es decir, estaba sujeto a dos conjuntos normativos mientras estaba sentado en esa silla.

Entonces, ¿qué normas se aplicarían? ¿Cómo abordarían los Estados del espacio real el conflicto entre estas dos comunidades?

Puede que algunos ejemplos ayuden a establecer un contexto en el que se pueda responder a estas preguntas. Por lo general, cuando un estadounidense va a Europa, no se lleva consigo al gobierno federal, ni tampoco acarrea un conjunto de reglas para los estadounidenses de viaje por Europa. Si va a Alemania, está generalmente sujeto a la ley alemana, y EEUU posee normalmente muy pocas razones para preocuparse de regular su conducta allí.

Pero a veces el gobierno de EEUU sí tiene una razón para regular a sus ciudadanos en el extranjero. Cuando es así, ninguna ley internacional puede detenerlo.[15] Por ejemplo, hay jurisdicciones donde la pedofilia no está adecuadamente regulada, y durante un tiempo se convirtieron en destinos turísticos predilectos de los pedófilos de todo el mundo. Esto llevó al gobierno de EEUU a promulgar una ley en 1994 que prohibía a los estadounidenses mantener relaciones sexuales con niños mientras estaban fuera del país, incluso en aquellas jurisdicciones donde el sexo con niños está permitido.[16]

---

15 Véase *Restatement (Third) of Foreign Relations Law*, 1986, 402(2) y comentario (e).

16 Child Sexual Abuse Prevention Act, 18 USC 2423(b), 1994. Véase Margaret A. Healy, «Prosecuting Child Sex Tourists at Home: Do Laws in Sweden, Australia, and the United States Safeguard the Rights of Children as Mandated by International Law?», *Fordham International Law Journal*, núm. 18, 1995, pp. 1852, 1902-1912.

¿Qué justificación podría haber para una ley así? Obviamente, el sentido que le daba el Congreso era que si ciudadanos estadounidenses incurrían en dicha conducta en un país extranjero, era más probable que hicieran lo mismo en EEUU. Si visitan una comunidad donde las normas permiten tal conducta, es más probable que traigan esas normas de vuelta a su vida en EEUU. Por lo tanto, aunque por lo general el gobierno estadounidense no se preocupa demasiado por lo que sus ciudadanos hagan en otros países, empieza a preocuparse cuando lo que hacen tiene consecuencias en su vida aquí.

Este tipo de regulaciones son excepcionales, por supuesto. Pero lo son porque la práctica de trasladarse a comunidades alternativas, o foráneas, del espacio real también es excepcional. La arquitectura del espacio real hace menos probable que las normas de una cultura foránea permeen la nuestra; la distancia entre ellas es tan grande que muy pocos pueden permitirse llevar una vida en ambos lugares.

Pero la Red cambia esto. Como sugiere el caso de Jake Baker, y como muchos otros revelarán apremiantemente, con la llegada del ciberespacio estas otras comunidades ya no están en otro lugar. Ahora se pueden traer aquí o, de forma más espeluznante, pueden *entrar* en nuestras casas. Las comunidades del espacio real ya no cuentan con el amortiguador de la arquitectura para protegerlas. Ahora otra comunidad puede captar la atención de sus ciudadanos sin que éstos lleguen jamás a salir de su habitación, ya que la gente puede estar en ambos lugares al mismo tiempo, y uno influye en el otro. Como escribe Edward Castronova: «Los mundos sintéticos se están volviendo importantes porque lo que ocurre dentro de ellos puede tener consecuencias fuera».[17] La cuestión que se le plantea al Estado es hasta qué punto dejar que lleguen estas consecuencias.

Lo cierto es que esta cuestión consta realmente de tres partes distintas —dos antiguas y una nueva. La primera parte antigua es hasta qué punto permitirá un Estado que lo extranjero influya en su cultura y en sus habitantes. Aquellas culturas aisladas en una época son posteriormente invadidas cuando caen sus barreras contra las invasiones. Pensemos en el alegato de los europeos en favor de detener la invasión de la cultura estadounidense, que mana a través de la televisión por satélite en las salas de estar de los ciudadanos europeos.[18]

---

17 Castronova, *Synthetic Worlds*, *op. cit.*, 2005, p. 7.

18 Véase Bill Grantham, «America the Menace: France's Feud With Hollywood», *World Policy Journal*, vol. 15, núm. 2, verano de 1998, p. 58; Chip Walker, «Can TV Save the Planet?», *American Demographics*, mayo de 1996, p. 42.

O en un caso aún más extremo, el de Oriente Medio. Estos lugares han luchado prolongadamente para proteger su cultura de ciertas influencias foráneas, y esa lucha se vuelve mucho más difícil una vez que Internet se hace ubicua.

La segunda parte antigua es la cuestión de si un Estado protegerá a sus ciudadanos de prácticas o reglas extranjeras incoherentes con las suyas, y cómo lo hará. Por ejemplo, la ley de derechos de autor en Francia protege fuertemente los «derechos morales» de los autores franceses. Si un autor francés suscribe un contrato con un editor estadounidense, y ese contrato no protege adecuadamente los derechos morales del ciudadano francés, ¿cómo responderá Francia?

La tercera cuestión —y la parte nueva— es la planteada por la capacidad de los ciudadanos de vivir en una cultura foránea al tiempo que siguen en casa. Esto supone algo más que meramente ver canales de televisión extranjeros, pues las alternativas que ofrece la televisión son alternativas de la imaginación. La vida interactiva del ciberespacio ofrece formas alternativas de vivir (al menos así lo hacen algunos ciberespacios).

En este capítulo mi atención no se centra en la primera cuestión, que muchos denominan imperialismo cultural, sino en los conflictos que se manifestarán respecto a las otras dos cuestiones. Muy probablemente sea cierto que siempre ha habido conflictos entre las reglas de distintos Estados; y puede que estos conflictos siempre hayan permeado las disputas locales particulares. Pero el ciberespacio ha hecho que estalle este tercer escenario de debate. Aquello que una vez constituyó la excepción se volverá la regla. La conducta que solía gobernarse en el seno de una jurisdicción, o de dos jurisdicciones coordinadas, ahora será sistemáticamente gobernada en jurisdicciones múltiples y descoordinadas. ¿Cómo puede la ley manejar esto?

La integración del ciberespacio producirá un tremendo incremento de la incidencia de estos conflictos al generar un tipo de conflicto que nunca antes se había dado: un conflicto planteado por individuos procedentes de diferentes jurisdicciones que conviven en un espacio al tiempo que viven en sus respectivas jurisdicciones.

Esta cuestión ha provocado una feroz discusión entre dos extremos. En uno de ellos está la obra de David Post y David Johnson. Johnson y Post sostienen que la multiplicidad de jurisdicciones a las que está sometida nuestra conducta (puesto que todo lo que hagamos en el ciberespacio afecta a todos los demás contextos) debería suponer que buena parte de ella no

esté presumiblemente regulada en ningún lugar; excepto, claro está, en el ciberespacio.[19] La incoherencia de cualquier otra solución, afirman, sería absurda. En lugar de abrazar el absurdo, deberíamos decantarnos por algo mucho más sensato: la vida en el ciberespacio, como Milan Kundera podría expresarlo, es vida en otro lugar.

En el otro extremo está la obra de eruditos como Jack Goldsmith y Tim Wu, quienes afirman que no hay nada nuevo aquí —al menos nuevo desde la perspectiva del Derecho Internacional Privado.[20] Según ellos, la ley lleva muchos años aplicándose a fondo con estos conflictos de autoridad. Puede que el ciberespacio aumente la incidencia de estos conflictos, pero no modifica su naturaleza; puede que haya que remodelar las viejas estructuras para adaptarlas a esta nueva forma, pero bastará con el molde antiguo.

Aunque ambos extremos tienen su parte de razón, en mi opinión los dos están equivocados. Es verdad, como Johnson y Post sostienen, que aquí hay algo nuevo; pero la novedad no radica en una diferencia de tipo sino de grado. Y es verdad, como Goldsmith y Wu sostienen, que siempre nos hemos enfrentado a disputas de esta índole, pero nunca a este nivel. Nunca hemos vivido una época en que pudiéramos afirmar que la gente vive efectivamente en dos lugares a la vez, sin principio de supremacía entre ellos. Éste es el desafío al que nos enfrentaremos en el futuro.

Esta dualidad constituye un problema porque las herramientas legales que venimos usando hasta ahora para resolver estas cuestiones no fueron diseñadas para abordar conflictos entre ciudadanos, sino entre instituciones, o actores relativamente sofisticados. Son reglas creadas para negocios que interactúan con otros negocios, o para negocios que interactúan con Estados. No son reglas diseñadas para disputas entre ciudadanos.

---

19 Véase, por ejemplo, David R. Johnson y David Post, «Law and Borders —The Rise of Law in Cyberspace», *Stanford Law Review*, núm. 48, 1996, pp. 1379-1380.

20 Jack Goldsmith y Timothy Wu, *Who Controls the Internet, op. cit.* Véase Jack L. Goldsmith, «Against Cyberanarchy», *University of Chicago Law Review*, núm. 65, 1998, p. 1199; Jack L. Goldsmith, «The Internet and the Abiding Significance of Territorial Sovereignty», *Indiana Journal of Global Legal Studies*, núm. 5, 1998, p. 475; véase también David Johnston, Sunny Handa y Charles Morgan, *Cyberlaw: What You Need to Know About Doing Business Online*, Toronto, Stoddart, 1997, cap. 10. En «The Unexceptional Problem of Jurisdiction in Cyberspace», *The International Lawyer*, núm. 32, 1998, p. 1167, Allan R. Stein arguye que los problemas jurisdiccionales en el ciberespacio son iguales a los que se encuentran en el Derecho Internacional del espacio real.

Jessica Litman plantea un argumento análogo en su obra sobre el copyright.[21] Durante buena parte del siglo pasado, afirma Litman, el copyright ha funcionado bastante bien como un acuerdo entre editores y autores. Se trata de una ley que se ha aplicado eminentemente a las instituciones, dejando fuera de su ámbito de aplicación a los individuos en tanto que éstos realmente no «editaban».

Internet, por supuesto, cambia todo esto: ahora todos somos editores. Y Litman sostiene (convincentemente, a mi ver) que las reglas del copyright no necesariamente funcionan bien cuando se aplican a los individuos.[22] Es posible que las reglas ideales para los individuos no sean necesariamente las ideales para las instituciones. Las reglas del copyright han de transformarse para adaptarlas mejor a un mundo donde los individuos también son editores.

Esto mismo es aplicable a los conflictos entre soberanos. Las reglas para abordar estos conflictos funcionan bien cuando las partes son «jugadores repetidos» —por ejemplo, empresas que deben hacer negocios en dos lugares, o individuos que viajan constantemente entre dos sitios. Estas personas pueden tomar medidas para conformar su conducta a la limitada gama de contextos donde viven, y las reglas existentes les ayudan a hacerlo. Pero de ahí no se desprende (como tampoco lo hace en el contexto del copyright) que la misma combinación de reglas fuera la mejor en un mundo donde cualquiera pudiese ser una multinacional.

La solución a este cambio no provendrá de insistir en que todo es lo mismo o en que todo es diferente; costará mucho más trabajo que eso. Cuando un gran número de ciudadanos vive en dos lugares distintos, y uno de estos lugares no está únicamente dentro de la jurisdicción de una soberanía concreta, ¿qué clase de reclamaciones debería poder hacer una soberanía frente a las demás, y qué clase de reclamaciones pueden hacer todas ellas al ciberespacio?

Aún no hay respuesta a esta pregunta. Se trata de otra ambigüedad latente en nuestro pasado constitucional —pero en este caso no hay un momento de fundación constitucional internacional al que atenerse. Incluso de haberse dado, no habría respondido a esta pregunta. En el

---

21 Véase Jessica Litman, «The Exclusive Right to Read», *Cardozo Arts and Entertainment Law Journal*, núm. 13, 1994, p. 29.

22 *Ibidem*.

momento en que se redactó la Constitución estadounidense, la gente común no vivía rutinariamente en múltiples jurisdicciones descoordinadas entre sí. Esto supone algo nuevo.

Posibles soluciones

Podemos estar seguros de que surgirán conflictos en torno al modo en que los Estados desean que se comporten sus ciudadanos. Lo que aún no es tan seguro es cómo se resolverán dichos conflictos. En esta sección, mapearé tres estrategias distintas: la primera fue el sueño de la Internet primigenia; la segunda es la realidad que muchas naciones contemplan hoy de manera creciente; y la tercera es el mundo en el que nos convertiremos poco a poco.

La regla de la ausencia de ley

El 8 de febrero de 1996, John Perry Barlow, ex letrista del grupo de rock Grateful Dead y cofundador de la Electronic Frontier Foundation, publicó esta declaración en la página web de la EFF:

> Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro, os pido a vosotros, que pertenecéis al pasado, que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía allí donde nos reunimos.
>
> No poseemos ningún gobierno electo, ni es probable que lleguemos a tenerlo, así que me dirijo a vosotros sin otra autoridad que aquélla con la que siempre habla la libertad. Declaro el espacio social mundial, que estamos construyendo, independiente por naturaleza de las tiranías que buscáis imponernos. No tenéis derecho moral alguno a gobernarnos ni poseéis tampoco ningún método para hacerlo que debamos temer en verdad.
>
> Los gobiernos derivan sus justos poderes del consentimiento de los que son gobernados. No habéis solicitado ni recibido el nuestro. No os hemos invitado. No nos conocéis, ni conocéis nuestro mundo. El ciberespacio no se

encuentra dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuese un proyecto de obras públicas. No podéis. Es un acto de la naturaleza que crece mediante nuestras acciones colectivas.

No habéis tomado parte en nuestra gran y creciente conversación, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que proporcionan ya más orden a nuestra sociedad del que podría obtenerse con cualquiera de vuestras imposiciones.

Proclamáis que hay problemas entre nosotros que necesitáis resolver. Usáis tal proclama como una excusa para invadir nuestros límites. Muchos de estos problemas no existen. Allí donde haya conflictos reales, allí donde haya errores, los identificaremos y abordaremos por nuestros propios medios. Estamos constituyendo nuestro propio Contrato Social. Esta forma de gobierno surgirá según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente.

El ciberespacio consta de transacciones, relaciones y del propio pensamiento, dispuestos como una onda estacionaria en la telaraña de nuestras comunicaciones. El nuestro es un mundo que está a la vez en todas partes y en ninguna, pero no está donde viven los cuerpos.

Estamos creando un mundo donde todos pueden entrar sin privilegios ni prejuicios determinados por la raza, el poder económico, la fuerza militar o la extracción social.

Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que éstas sean, sin miedo a verse compelido al silencio o la conformidad.

Vuestros conceptos legales de propiedad, expresión, identidad, movimiento y contexto no se nos pueden aplicar. Todos ellos se basan en la materia, y aquí no hay materia.

Nuestras identidades no tienen cuerpo, por lo que, a diferencia de vosotros, no podemos lograr el orden mediante coerción física. Creemos que nuestra forma de gobierno surgirá de la ética, de un interés propio bien informado y del bien común. Nuestras identidades pueden distribuirse a través de muchas de vuestras jurisdicciones. La única ley que todas nuestras culturas constituyentes reconocerían es la Regla de Oro. Esperamos ser capaces de construir nuestras soluciones particulares sobre esa base. Pero no podemos aceptar las soluciones que estáis tratando de imponer.

En Estados Unidos, hoy habéis creado una ley, la Ley de Reforma de las Telecomunicaciones, que repudia vuestra propia Constitución e insulta los sueños de Jefferson, Washington, Mill, Madison, de Toqueville y Brandeis. Estos sueños deben renacer ahora en nosotros.

Os aterrorizan vuestros propios hijos, puesto que son nativos de un mundo donde vosotros siempre seréis inmigrantes. Como les teméis, encomendáis a vuestra burocracia las responsabilidades paternas a las que sois demasiado

> cobardes para enfrentaros vosotros mismos. En nuestro mundo, todos los sentimientos y expresiones de humanidad, de las más degradantes a las más angelicales, son parte de un todo fluido, la conversación mundial de bits. No podemos separar el aire que asfixia del aire en el que se baten las alas.
>
> En China, Alemania, Francia, Rusia, Singapur, Italia y Estados Unidos, estáis intentando conjurar el virus de la libertad erigiendo puestos de guardia en las fronteras del ciberespacio. Puede que impidan el contagio durante un breve lapso, pero no funcionarán en un mundo que pronto estará cubierto de medios que transmiten bits.
>
> Vuestras industrias de información cada vez más obsoletas se perpetuarían a sí mismas proponiendo leyes, en Estados Unidos y en otros sitios, que afirmen que son los dueños de la expresión misma a escala mundial. Estas leyes declararían que las ideas son otro producto industrial, no más noble que el hierro en lingotes. En nuestro mundo, cualquier cosa que pueda crear la mente humana puede ser reproducida y distribuida infinitamente sin ningún coste. El trasvase mundial del pensamiento ya no necesita vuestras fábricas para llevarse a cabo.
>
> Estas medidas cada vez más hostiles y coloniales nos sitúan en la misma posición que aquellos precedentes amantes de la libertad y la autodeterminación que tuvieron que rechazar la autoridad de poderes lejanos e ignorantes. Debemos declarar nuestros «yoes» virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro dominio sobre nuestros cuerpos. Nos desplegaremos a través del planeta para que nadie pueda apresar nuestros pensamientos.
>
> Crearemos una civilización de la mente en el ciberespacio. Ojalá sea más humana y justa que el mundo que vuestros gobiernos han creado antes.[23]

Quizá no exista un documento que refleje mejor el ideal dominante en la Red hace una década. Cualquiera que fuera el dominio ejercido sobre «nuestros cuerpos», ningún gobierno podría regir los «yoes virtuales» que habitarían en este espacio. Barlow declaró a estos «yoes virtuales» «inmunes» a los soberanos del espacio real, que estarían perdidos si trataban de ejercer su control en el ciberespacio.

Aunque Barlow lanzó su declaración en una cumbre de líderes mundiales en Davos, aparentemente los gobiernos del mundo no oyeron lo que dijo. El mismo 8 de febrero de 1996 el presidente Clinton aprobó la «Ley de Decencia en las Comunicaciones».[24] Y aunque el Tribunal Supremo finalmente revocó la

---

23 Véase John Perry Barlow, «A Declaration of the Independence of Cyberspace», 1996, disponible en http://homes.eff.org/~barlow/Declaration-Final.html [disponible en castellano en http://biblioweb.sindominio.net/telematica/manif_barlow.html].

24 Véase *Communications Decency Act*, PL 104-104, 110 Stat. 56 (1996).

ley, ni mucho menos cerró la puerta a la regulación de los «yoes virtuales». Un rosario de leyes procedentes del Congreso estadounidense coincidió con un rosario de regulaciones procedente del resto del mundo; y esa tendencia no ha hecho más que acentuarse. Tal como midió un estudio, el aumento de iniciativas legislativas para regular la Red fue lento al principio, pero ha despegado drásticamente.[25] Estas regulaciones se encaminaron en primer lugar a «aprovechar la tecnología para servir a lo que se percibía como objetivos gubernamentales no relacionados con la red»; en segundo lugar iban «orientadas directamente a fomentar el avance de la infraestructura de la Red»; y en tercer lugar «implicaban directamente el control sobre la información».[26]

Las razones por las que los ideales de Barlow no iban a hacerse realidad podrían parecer obvias retrospectivamente, pero en aquel momento no se las reconoció bien. Las leyes se promulgan como resultado de la acción política; y asimismo pueden detenerse sólo por medio de la acción política. Las ideas, o la buena retórica, no constituyen acciones políticas. Cuando el Congreso se enfrenta a padres enardecidos que le demandan que haga algo para proteger a sus hijos en la Red; o cuando aparecen músicos de fama mundial indignados con las infracciones del copyright en la Red; o cuando se encuentra con agentes gubernamentales de aire circunspecto que le hablan de los peligros del crimen en la Red, ni siquiera la retórica de un letrista de Grateful Dead servirá de gran cosa. Por el lado de Barlow tenía que emprenderse también acción política, pero la acción política era precisamente aquello para lo que la red no estaba preparada.

La regla de una sola ley

El resultado opuesto a la ausencia de ley es un mundo donde no existe más que una ley. Se trata de un mundo donde un Estado (o acaso todos ellos trabajando conjuntamente, aunque esta idea resulta demasiado ridícula para contemplarla siquiera, por lo que no la discutiré aquí) domina el mundo mediante la aplicación de sus leyes por doquier.

---

25 Yochai Benkler, «Net Regulation: Taking Stock and Looking Forward», *University of Colorado Law Review*, núm. 71, 2000, pp. 1203, 1206–07.

26 *Ibidem*, pp. 1203, 1232, 1234, 1237.

Como Michael Geist argumenta convincentemente, eso es exactamente lo que está ocurriendo en la actualidad. «Los Estados», escribe Geist, son «reacios a reconocer que las leyes nacionales se circunscriben a las fronteras nacionales, y están recurriendo cada vez más a una legislación explícitamente extraterritorial».[27]

En esto también (por desgracia), EEUU va en cabeza. EEUU posee una opinión sobre la conducta adecuada en la red y ha reclamado el derecho a aplicarla extraterritorialmente, de modo que aplica sus reglas contra ciudadanos de todo el mundo sin importar que dichas reglas colisionen con las locales. A la Comisión Federal de Comercio, por ejemplo, se le «atribuye la responsabilidad de aplicar la Ley de Protección de la Privacidad Infantil en Internet», escribe Geist, y «su orientación reglamentaria no deja lugar a dudas de que se espera que tales sitios cumplan con el estatuto en sus prácticas de privacidad con respecto a los niños».[28] También el Departamento de Justicia mantiene que la Ley de Copyright del Milenio Digital es de aplicación extraterritorial, ya que se refiere a «importaciones» de tecnología.[29] Y la Ley Patriótica de EEUU incluye disposiciones que son «expresamente extraterritoriales» —incluyendo, por ejemplo, una expansión de la lista de «ordenadores protegidos» que alcanza a «un ordenador situado fuera de EEUU que se use de un modo que afecte al comercio o a la comunicación interestatales o internacionales de EEUU».[30]

Por supuesto, Geist no defiende que EEUU haya sometido Internet. Nadie afirmaría que EEUU ha acabado con el crimen en la Red, ni tan siquiera con la conducta contraria a la legislación estadounidense. Pero la actitud y la teoría que animan el enjuiciamiento en EEUU carecen de límites conceptuales. Según la teoría que promueve EEUU, no existe ninguna conducta en ninguna parte que, al menos en principio, quede fuera del alcance de los tribunales estadounidenses. (No obstante, muchos creen que el Derecho Internacional restringe a EEUU más de lo que éste reconoce).[31]

---

27 Michael Geist, «Cyberlaw 2.0», *Boston College Law Review*, núm. 44, 2003, pp. 323, 332. Para un argumento relacionado, véase Matthew Fagin, «Regulating Speech Across Borders: Technology vs. Values», *Michigan Telecommunications Technology Law Review*, núm. 9, 2003, p. 395.

28 Geist, *ibidem*, p. 343.

29 *Ibidem*, p. 338.

30 *Ibidem*, pp. 344-345.

31 Patricia L. Bellia, «Chasing Bits Across Borders», *University of Chicago Legal Forum*, núm. 35, 2001, p. 100.

Puede que esta supremacía estadounidense continúe para siempre, pero yo lo dudo. Hay un deseo creciente entre muchos Estados del mundo de contener el poder de EEUU. En 2005 algunos de ellos intentaron arrebatarle el control de ICANN (Internet Corporation for Assigned Names and Numbers, Corporación de Internet para la Asignación de Nombres y Números). Esta resistencia, unida a una sana dosis de dignidad soberana, impulsará cada vez más un régimen que equilibre mejor los intereses del mundo en su conjunto.

La regla de múltiples leyes (y la tecnología para posibilitarla)

Entonces, ¿cómo sería un régimen más equilibrado?

Retomemos el conflicto expuesto al principio de este capítulo. Por un lado, Francia no quiere que sus ciudadanos compren parafernalia nazi, y EEUU no quiere que sus ciudadanos vean televisión «gratis». Por otro lado, Francia no tiene nada contra la televisión «gratis», y EEUU no dispone del poder constitucional para impedir a sus ciudadanos comprar parafernalia nazi. ¿Hay algún modo de dar a Francia lo que quiere (y no quiere) y a EEUU lo que quiere (y no puede querer)?

Ésta no es una cuestión limitada a Francia y EEUU. Como Victor Mayer-Schonberger y Teree Foster han escrito acerca de la regulación de la expresión:

> Las restricciones nacionales a la libertad de expresión en Internet constituyen un lugar común no sólo en EEUU, sino también en todo el mundo. Las naciones, cada cual resuelta a custodiar lo que perciben que está dentro de los márgenes de sus intereses nacionales, buscan regular ciertas formas de expresión debido a contenidos considerados reprensibles u ofensivos al bienestar o a la virtud cívica nacional.[32]

¿Hay una solución general (al menos a ojos de los Estados) a este problema?

32 Viktor Mayer-Schonberger y Teree E. Foster, «A Regulatory Web: Free Speech and the Global Information Infrastructure», *Michigan Telecommunications and Technology Law Review*, vol. 3, núm. 45, 1997.

Bien, en primer lugar imaginémonos que se afianza algo similar a la Capa de Identidad descrita en el Capítulo 4, y que ésta conlleva que los individuos pueden certificar (con facilidad y sin revelar necesariamente nada más) su ciudadanía. De este modo, cuando alguien navega por la Red, su presencia lleva anexa un objeto criptográfico que revela, como mínimo, a qué jurisdicción está sujeto.

En segundo lugar, imaginémonos una convención internacional para completar una tabla con todas las reglas que cada Estado quiere aplicar a sus ciudadanos mientras se hallen en el extranjero. Así, por ejemplo, los franceses querrían bloquear el material nazi; los estadounidenses, la pornografía para menores de dieciocho años, etc. A continuación, la tabla se publicaría y se pondría a disposición de cualquier servidor de Internet.

Finalmente, imaginémonos que los Estados comienzan a exigir que los servidores dentro de su jurisdicción respeten las reglas expresadas en la tabla. De esta manera, si un sitio web ofrece material nazi y una ciudadana francesa entra en él, el sitio debería bloquearle el acceso; pero si la que entra es ciudadana estadounidense, puede acceder normalmente. En consecuencia, cada Estado restringiría a los ciudadanos extranjeros como sus respectivos Estados quisieran, pero sus ciudadanos disfrutarían de las libertades que esa nación garantiza. Tal mundo implantaría, pues, las reglas locales en la vida del ciberespacio.

Consideremos un ejemplo concreto para clarificar esta dinámica: el juego.[33] El Estado de Minnesota posee una política estatal restrictiva respecto a los juegos de azar.[34] El legislador de Minnesota ha prohibido jugar a sus ciudadanos, y su Fiscal General ha aplicado vigorosamente tal prohibición legislativa —tanto clausurando los sitios de juegos radicados en Minnesota como amenazando con emprender acciones legales contra los sitios de fuera del Estado que permitan jugar a sus ciudadanos.

33 Describo este ejemplo a escala estatal, pero el régimen que estoy imaginando funcionaría en el ámbito de los Estados-nación, no de los Estados que conforman EEUU.

34 Véase Minnesota Statute 609.75, subd. 2-3, 609.755, 1, 1994, que tipifica como falta realizar una apuesta a menos que se haga a través de una actividad exenta y regulada por el Estado, como los sorteos benéficos autorizados o la lotería estatal. Las organizaciones de juego a través de Internet no quedan exentas de esta norma.

Tal amenaza, aducirán algunos, no puede tener efecto alguno sobre el juego en Internet, ni sobre las apuestas de los ciudadanos de Minnesota.[35] La prueba es la historia de Boral: imaginémonos un servidor de juego radicado en Minnesota que, cuando este Estado ilegaliza el juego, puede trasladarse a otro lugar. Desde el punto de vista de los ciudadanos de Minnesota, el cambio (apenas) tiene consecuencias, ya que tan sencillo es acceder a un servidor localizado en Minneapolis como hacerlo a uno localizado en Chicago. Así pues, el sitio de juego puede trasladarse fácilmente y conservar a todos sus clientes de Minnesota.

Supongamos que Minnesota amenaza entonces con procesar al dueño del servidor de Chicago. Para el Fiscal General de Minnesota, resulta relativamente fácil persuadir a los tribunales del Estado de Illinois para que procesen al servidor ilegal de Chicago (suponiendo que pudiera demostrarse que el comportamiento del servidor era de hecho ilegal). Ante ello el servidor se limita a trasladarse de Chicago a las Islas Caimán, poniendo una barrera más a su procesamiento por el Estado de Minnesota sin dificultar ni un ápice el acceso de sus ciudadanos al juego. Por más que se esfuerzan las autoridades de Minnesota, parece que la Red ayuda a sus ciudadanos a eludir a su Estado. La Red, ajena a la geografía, hace prácticamente imposible que los Estados geográficamente limitados apliquen sus reglas.

Imaginémonos ahora, sin embargo, la Capa de Identidad que describí más arriba, en la que todo el mundo puede certificar su ciudadanía de forma automática (y sencilla). Al entrar en un sitio web, éste comprueba nuestro documento de identidad, con lo que un sitio de juego podría empezar a condicionar el acceso en función de si poseemos el documento de identidad adecuado para él —si somos de Minnesota y se trata de un sitio de juego, éste no nos deja pasar. Este proceso se da de forma invisible, entre ordenadores. Lo único que sabemos es que se nos permite acceder, y si no es así, entonces se nos indica por qué no.[36]

En esta historia, pues, se respetan los intereses del Estado de Minnesota y no se permite jugar a sus ciudadanos. Pero los deseos del Estado de Minnesota no determinan las prácticas de juego de quienes no viven en ese Estado: sólo los ciudadanos de Minnesota se ven afectados por esta regulación.

---

35 Véase Scott M. Montpas, «Gambling Online: For a Hundred Dollars, I Bet You Govern ment Regulation Will Not Stop the Newest Form of Gambling», *University of Dayton Law Review*, núm. 22, 1996, p. 163.

36 O al menos podría funcionar así. Dependiendo del diseño, podría revelar mucha más información.

Estamos ante una regulación a escala estatal y relativa a un solo problema. Pero, ¿por qué los demás Estados de EEUU cooperarían con Minnesota? ¿Por qué las autoridades de cualquier otra jurisdicción querrían cumplir la regulación de Minnesota?

La respuesta es que no querrían si ésta fuera la única regulación en juego. Pero no lo es. El Estado de Minnesota quiere proteger a sus ciudadanos del juego, pero el de Nueva York puede querer hacer lo propio respecto del abuso de los datos privados; la Unión Europea puede compartir el objetivo de Nueva York, y el Estado de Utah puede compartir el de Minnesota.

En otras palabras, cada Estado tiene sus propios intereses en controlar ciertas conductas, y estas conductas difieren. Pero la clave es ésta: la misma arquitectura que permite al Estado de Minnesota alcanzar su propósito regulador puede también ayudar a otros estados a alcanzar los suyos propios. Y ello puede dar a pie a una especie de *quid pro quo* entre jurisdicciones.

El pacto sería algo así: cada Estado prometería imponer a los servidores dentro de su jurisdicción las regulaciones que otros Estados aplican a sus ciudadanos, a cambio de que estos Estados hagan lo propio con las suyas. Así, las autoridades de Nueva York exigirían a los servidores dentro de su jurisdicción que impidan el acceso al juego a los ciudadanos de Minnesota; a cambio, las autoridades de Minnesota excluirían a los ciudadanos neoyorquinos de los servidores que explotan la privacidad. Del mismo modo, el Estado de Utah excluiría a los ciudadanos de la Unión Europea de los servidores que explotan la privacidad a cambio de que la Unión Europea impidiera a los ciudadanos de Utah acceder a los sitios europeos de juego.

De hecho, ésta es precisamente la estructura que ya está implantada en EEUU para regular el juego interestatal. Según la legislación federal, el juego interestatal a través de Internet está prohibido a menos que los usuarios procedan de un Estado donde se permite el juego y se conecten a un servidor radicado en un Estado donde también esté permitido.[37] Si en el Estado del que proceden o al que se conectan el juego está prohibido, los usuarios cometen un delito federal.

---

37 Véase 18 USC 1955, que regula los negocios y define «juego ilegal» interestatal como aquél que se da en un Estado donde el juego es ilegal.

Esta misma estructura podría usarse para respaldar la regulación local de la conducta en Internet. En efecto, contando con un modo sencillo de verificar la ciudadanía, un modo sencillo de verificar que los servidores están discriminando en función de ella y un compromiso federal de respaldar esta discriminación local, podríamos imaginar una arquitectura que posibilite la regulación local de la conducta en Internet.

Y si todo esto puede darse en el seno de EEUU, podría darse de forma general entre las naciones. En el ámbito internacional, el interés en hacer cumplir las leyes locales es igual que en el nacional —quizá incluso mayor. Por lo tanto, una Internet rica en documentos de identidad facilitaría la zonificación y posibilitaría esta estructura de control internacional.

Un régimen de esta índole restituiría la zonificación geográfica en la Red, restableciendo las fronteras en una red construida sin ellas. Tal régimen otorgaría a los reguladores de Hungría y Tailandia el poder para hacer aquello que ahora mismo no pueden —controlar a sus ciudadanos a su antojo—, y dejaría tanta libertad a los ciudadanos estadounidenses o suecos como sus respectivos gobiernos han determinado que les corresponde.

Para los amantes de la libertad de la Red original, este régimen es una pesadilla, pues elimina la libertad creada por la arquitectura de Internet y restaura el poder de controlar en un espacio diseñado para evitar el control.

Yo también amo la libertad de la Internet original. Pero dado que me he vuelto escéptico acerca de los atajos hacia las políticas que me gustan —por atajos entiendo aquellos dispositivos que producen un resultado particular sin respaldo democrático efectivo— me siento indeciso a la hora de condenar este régimen. Por supuesto, ningún régimen democrático debería permitir que la voluntad de un Estado no democrático quede reflejada en una tabla de zonificación; no deberíamos ayudar a los regímenes totalitarios a reprimir a sus ciudadanos. Ahora bien, en el seno de una familia de Estados democráticos, tal régimen podría contribuir a promover la democracia. Y si a la gente le disgusta una restricción sobre la libertad, dejemos que se movilicen para eliminarla.

Por supuesto, mi visión es que los ciudadanos de cualquier democracia deberían tener la libertad de elegir qué discursos consumen; pero preferiría que se ganaran tal libertad demandándola a través de medios democráticos a que un truco tecnológico se la diera gratuitamente.

Pero independientemente de si este régimen gusta o no al lector, o a mí, mi argumento en este momento tiene un carácter de predicción. Este régimen supone un acuerdo natural entre dos resultados que los Estados no aceptan —éstos no aceptarán ni un mundo donde las leyes del espacio real no influyan en el ciberespacio, ni uno donde las normas de un Estado, o de unos pocos Estados, controlen el mundo. Este régimen concede a cada Estado el poder de regular a sus ciudadanos; ningún Estado debería tener derecho a hacer nada más.

Tal equilibrio ya se ha alcanzado en la Red de forma privada —por más que haya una resistencia y un malestar significativos al respecto. Como ya he descrito, en enero del 2005, Google anunció que iba a dar al Estado chino algo que se había negado a dar a nadie más en el mundo —una versión del motor de búsqueda de Google que bloquea el contenido que el Estado chino no quiere que vean sus ciudadanos.[38] De este modo, si buscamos «democracia» o «derechos humanos» en Google.cn, no encontraremos aquello que encontramos si lo buscamos en Google.com. (En este momento Wikipedia mantiene una lista de palabras bloqueadas por los motores de búsqueda en China).[39] Por lo tanto, Google reconstruirá Internet para los ciudadanos chinos, en la práctica, de acuerdo con los principios que promueve el Estado chino.

Comprendo el motivo de Google (el beneficio), y ciertamente comprendo su justificación (ello impulsará a China hacia una verdadera democracia). Ahora bien, creamos o no que este equilibrio es justo en el contexto de la China comunista, ciertamente tiene más justificación cuando describimos acuerdos entre naciones democráticas. A mi juicio, la forma en que el Estado chino trata a sus periodistas está mal; y si un editor chino me ofreciera publicar este libro en China con la sola condición de que omitiera este párrafo, ciertamente me negaría. Pero mi punto de vista es diferente cuando se trata de reglas impuestas por Francia o Italia.

Una consecuencia importante de esta arquitectura —es más, quizá una razón suficiente para oponerse a ella— es que facilitará la regulación; y cuanto más fácil es regular, más probabilidades hay de que se introduzca la regulación.

---

38 Como describí más arriba, véase supra, Capítulo 5, nota 38, seis meses después de tomar esta decisión, uno de los fundadores de Google estaba sintiendo remordimientos. Véase Clive Thompson, «Google's China Problem (And China's Google Problem)», *New York Times*, 23 de abril de 2006, sección 6, p. 64.

39 Véase Wikipedia, «List of Words Censored by Search Engines in Mainland China», disponible en http://en.wikipedia.org/wiki/List_of_words_blocked_by_search_engines_in_Mainland_China.

No obstante, ésta es la compensación —entre el coste y la buena voluntad de regular— que hemos visto una y otra vez. Lo que para el Estado es un coste para nosotros supone libertad, de modo que cuanto más cueste la regulación, menos probable es que se imponga. La libertad depende de que la regulación siga resultando cara. La libertad lleva aparejada un coste.

Cuando la regulación se vuelve sencilla o barata, sin embargo, esta libertad contingente corre riesgo, pues es de esperar que haya más regulaciones. En estos casos, si queremos conservar la libertad, tendremos que desarrollar argumentos afirmativos a su favor, con el fin de impedir la regulación de la Red basada en la identidad. Tal como explico en lo que queda de este libro, se da la coincidencia de un deseo sorprendentemente intenso de que la naciones adopten regímenes que faciliten la regulación específica por jurisdicciones y de una razón significativa por la que es probable que caigan los costes de la regulación. Deberíamos esperar, pues, que se impongan más regulaciones de este tipo. Y pronto.

El resultado sería, en síntesis, la zonificación del ciberespacio en función de los certificados que porten los usuarios individuales. Tal zonificación posibilitaría un grado de control del ciberespacio como pocos han imaginado jamás. El ciberespacio pasaría de ser un espacio irregulable a ser, dependiendo de la profundidad de los certificados, el espacio más regulable que se pueda imaginar.

Quinta parte

Respuestas

El argumento de la Primera Parte era que la irregulabilidad de la Internet original desaparecerá con el desarrollo de arquitecturas que hagan que la conducta en ella sea de nuevo regulable. La Segunda Parte describió un aspecto de esa regulabilidad —la tecnología. El «código» va a ser una parte cada vez más importante de esa regulación, aplicando directamente el control que la ley impone habitualmente por medio de amenazas. A continuación, la Tercera Parte examinó tres contextos en los que el cambio tecnológico tornaría ambiguos nuestros compromisos con ciertos principios fundamentales. Esto es lo que denominé una ambigüedad latente. El modo de proteger la propiedad intelectual, la privacidad o la libertad de expresión dependerá de decisiones fundamentales que los redactores de nuestra Constitución no tomaron. Después, la Cuarta Parte mapeó este conflicto con respecto a las jurisdicciones, con lo cual la lección retornaba nuevamente a la Primera Parte: la tendencia estatal impulsará una red cada vez más regulable, en esta ocasión para restituir las zonas geográficas en una Internet sin fronteras.

A lo largo de estas cuatro partes, mi objetivo central ha sido apremiar a reconocer algo que resulta obvio una vez observado: que hemos de tomar decisiones acerca de la evolución de la Red. Estas decisiones influirán de manera fundamental sobre qué valores se construyen en ella.

La cuestión que abordo en esta parte es si seremos capaces de tomar esas decisiones. Mi argumento es que no lo seremos. Hemos delegado tan completamente cuestiones de principios en el poder judicial, y hemos corrompido hasta tal extremo nuestro proceso legislativo con el reparto de dádivas bajo cuerda, que afrontamos este momento de extraordinaria importancia incapaces de tomar ninguna decisión útil. Se nos ha cogido con la guardia baja, ebrios de la indulgencia política de la época, y puede que lo máximo que seamos capaces de hacer sea tenernos en pie hasta que tengamos tiempo de recobrar la sobriedad.

16. Los problemas que afrontamos

HAY DECISIONES QUE DETERMINARÁN CÓMO ES EL CIBERESPACIO pero, a mi modo de ver, los estadounidenses no estamos capacitados para tomarlas. Y ello por tres razones muy distintas: la primera está ligada a los límites que imponemos a los tribunales; la segunda, a los límites que hemos descubierto en el poder legislativo; y la tercera, a los límites de nuestro pensamiento sobre el código. Si debe tomarse una decisión, estos límites indican que no lo haremos. Estamos en un momento en que se están tomando las decisiones más importantes acerca de cómo será este espacio, pero carecemos de las instituciones, o de la práctica, para evaluarlas o alterarlas fácilmente.

En el presente capítulo describo estos problemas, y en el Capítulo 17 bosquejo tres soluciones. Ninguna descripción será completa pero todas deberían darnos qué pensar. Los problemas que revela el ciberespacio no son problemas con el ciberespacio, sino problemas del espacio real que el ciberespacio nos muestra y que ahora debemos resolver —o quizá reconsiderar.

Problemas con los tribunales

Existen dos tipos de constituciones, una que podríamos denominar codificadora y otra que podríamos llamar transformadora. Una constitución codificadora trata de preservar algo esencial de la cultura constitucional o legal en la cual es promulgada —a fin de proteger ese atributo cultural de cambios futuros. Una constitución transformadora (o una enmienda) hace lo contrario:

trata de modificar algo esencial de la cultura constitucional o legal en la que es promulgada —para hacer que la vida sea diferente en el futuro, para rehacer alguna parte de la cultura. El símbolo del régimen codificador es Ulises atado al mástil; el símbolo del régimen transformador es la Francia revolucionaria.

Nuestra Constitución contiene ambos regímenes. La Constitución de 1789 —antes de introducir las primeras diez enmiendas— era una constitución transformadora, ya que «traía a la vida» una nueva forma de gobierno y daba origen a una nación.[1] La Constitución de 1791 —la Declaración de Derechos— era una constitución codificadora, pues con el trasfondo de la nueva constitución, buscaba afianzar ciertos principios frente a cambios futuros.[2] Las conocidas como «Enmiendas de la Guerra Civil» fueron nuevamente transformadoras, al proponerse reelaborar parte de aquello en lo que la cultura social y legal estadounidense se había convertido —con el fin de arrancar del alma estadounidense una tradición de desigualdad y reemplazarla por una tradición y práctica de igualdad.[3]

De estos dos regímenes, el transformador es claramente el más difícil de realizar. Un régimen codificador al menos tiene la inercia de su parte, mientras que un régimen transformador debe luchar; el régimen codificador cuenta con un momento de autoafirmación, mientras que el régimen transformador vive atormentado por las dudas y vulnerable a los intentos de socavarlo por parte de la oposición. Los momentos constitucionales mueren, y cuando lo hacen, las instituciones encargadas de hacer respetar sus mandatos, como los tribunales, se enfrentan a una creciente resistencia política. A pesar de los destellos de iluminación [*enlightenment*], la gente mantiene o retorna a sus viejos hábitos, y los tribunales encuentran dificultades para resistirse a esta tendencia.

---

1 *Missouri vs. Holland*, 252, US 416, 433, 1920.

2 Véase, por ejemplo, Jack N. Rakove, *Original Meanings: Politics and Ideas in the Making of the Constitution*, Nueva York, Alfred A. Knopf, 1996, pp. 289-290; véase también Akhil Reed Amar, «The Bill of Rights as a Constitution», *Yale Law Journal*, núm. 100, 1991, p. 1131, para otra interpretación similar de la Declaración de Derechos.

3 Esto no supone negar que algunos aspectos de la igualdad delineada en las Enmiendas de la Guerra Civil resonaban ya en nuestro pasado constitucional. Los abolicionistas, por supuesto, hicieron mucho hincapié en la reivindicación de igualdad de la Declaración de la Independencia; véase, por ejemplo, Trisha Olson, «The Natural Law Foundation of the Privileges or Immunities Clause of the Fourteenth Amendment», *Arkansas Law Review*, núm. 48, 1995, pp. 347, 364. Una enmienda puede ser transformadora, sin embargo, incluso si se limita a rememorar una parte del pasado y a restablecerla —como, por ejemplo, hizo Alemania tras la Segunda Guerra Mundial.

La propia historia constitucional de EEUU revela exactamente esta pauta. El momento extraordinario que se produjo tras la Guerra Civil —cuando se incorporaron al alma de la Constitución estadounidense tres enmiendas comprometidas con la igualdad civil— había pasado ya en 1875, momento en que la nación abandonó la lucha por la igualdad y se volcó en la agitación de la Revolución Industrial. Se ratificaron entonces leyes que imponían la segregación racial,[4] se negó a los afroamericanos el derecho al voto[5] y se permitieron leyes que implantaban lo que luego se comprobó que era un nuevo tipo de esclavitud.[6] Sólo al cabo de cien años de persistente desigualdad, el Tribunal Supremo hizo suya la causa de las Enmiendas de la Guerra Civil. Así, no sería hasta el caso «Brown contra la Junta de Educación», en 1954, cuando el Supremo reconoció de nuevo la idea transformadora de las Enmiendas de la Guerra Civil.[7]

Podría criticarse al Tribunal Supremo por este siglo de debilidad, pero creo que es más importante comprender la fuente de dicha debilidad. Los tribunales operan en el seno de un contexto político y dentro del mismo constituyen la instancia de resistencia más débil. Durante un tiempo pueden tener capacidad de insistir en un principio que está por encima del momento, pero ese tiempo acaba pasando. Si el mundo no reconoce lo negativas que son sus actitudes racistas, ni siquiera una contundente declaración de principios promulgada en la Constitución permite a un tribunal demasiada libertad para resistirse. Los tribunales están sujetos a las restricciones de lo que «todo el mundo» con voz y recursos para hacerse oír cree que es justo, por más que lo que «todo el mundo» cree sea incoherente con los textos constitucionales básicos.

La vida es más sencilla con una constitución codificadora, ya que existe una tradición que el texto ha de limitarse a afianzar. Y si dicha tradición viene de antiguo, entonces hay esperanza de que también permanezca sólida.

Ahora bien, incluso una constitución codificadora afronta dificultades. A pesar de la codificación, si las pasiones de una nación se vuelven lo bastante fuertes, los tribunales suelen estar dispuestos a hacer muy poco.

---

4 Véase *Plessy vs. Ferguson,* 163 US, nº 537, 1896.

5 Véase A. Leon Higginbotham Jr., «Racism in American and South African Courts: Similarities and Differences», *New York University Law Review*, núm. 65, 1990, pp. 479, 495-496.

6 Estas leyes permitían los trabajos forzados para pagar una deuda; véase *Bailey vs. Alabama,* 219 US, nº 219, 1911, que deroga las leyes de peonaje en virtud de la Decimotercera Enmienda.

7 *Brown vs. Board of Education*, 347 US, nº 483, 1954.

Así, pese a la claridad de la protección de la libertad de expresión consagrada en la Primera Enmienda, cuando se trataba de la expresión de comunistas y anarquistas, se permitía al Estado ejercer su poder para castigarla.[8] Y a pesar de la presunción de inocencia y de la igualdad, cuando Japón bombardeó Pearl Harbor, se permitió al Estado trasladar a todos los estadounidenses de origen japonés de la Costa Oeste de EEUU a campos de concentración.[9]

He aquí algunas realidades de los tribunales en un sistema democrático. A nosotros los abogados nos gusta idealizarlos, imaginarlos por encima de cualquier influencia. Pero nunca han sido así, de forma completa o permanente, pues están sujetos a una restricción política importante. Al fin y al cabo, no dejan de ser una institución en el seno de una democracia, y como tal no puede enemistarse con el pueblo durante mucho tiempo.

Es sobre este trasfondo sobre el que deberíamos reflexionar acerca de los problemas suscitados en las Partes Tercera y Cuarta. En cada uno de los casos, mi argumento era que necesitaremos elegir los principios que deseamos que abrace el ciberespacio, pues ningún texto constitucional o tradición trató estas cuestiones. Por lo general, tales cuestiones afectan a la parte codificadora de nuestra tradición, pero también constituyen casos de ambigüedad latente. No hay una «respuesta» en el sentido de un criterio que parezca establecido y que los tribunales puedan limitarse a adoptar. Por consiguiente, dicha respuesta debe ser elaborada, no encontrada; construida, no descubierta; elegida, no adoptada.

Esto crea dificultades a cualquier tribunal estadounidense. Vivimos a la sombra del Tribunal Supremo que presidió el juez Earl Warren. Muchos piensan (yo no me cuento entre ellos) que el suyo fue un tribunal frenéticamente activista que «se inventó» el Derecho Constitucional e impuso sus propios «principios personales» en el sistema político y legal. Y muchos vieron la etapa de presidente del Supremo del juez Rehnquist como un contrapeso a aquel activismo de antaño.

Yo creo que tal visión es errónea. El Tribunal Warren no era «activista» en ningún sentido que implique incoherencia con el principio de fidelidad interpretativa, y el Tribunal Rehnquist no era menos activista en ese mismo sentido que su predecesor. No obstante, la cuestión no es cuál es la verdad, sino qué cree la gente. Y lo que creemos es que el pasado estuvo marcado por el activismo, y que ese activismo era erróneo.

---

8 Véase, por ejemplo, *Dennis vs. United States,* 341 US, nº 494, 1951, donde se ratifican las condenas según la Ley Smith, que prohibía ciertas actividades del Partido Comunista.

9 Véase *Korematsu vs. United States*, 323 US, nº 214, 1944.

Erróneo al menos para un tribunal. Los opositores al Tribunal Warren no sólo son conservadores; también hay progresistas convencidos de que ese Tribunal no actuaba judicialmente,[10] de que estaba inventando, y no interpretando, el Derecho Constitucional —guiándose exclusivamente por el criterio de si podía conseguir una mayoría.

Cualquier tribunal corre el riesgo de parecerse al Tribunal Warren cuando dicta sentencias que no parecen emanar directa u obviamente de un texto legal. Cualquier tribunal es vulnerable cuando sus sentencias parecen políticas. Teniendo en cuenta los antecedentes históricos, nuestro Tribunal Supremo es particularmente vulnerable a esta visión, y se mostrará sensible a las reacciones cuando sus acciones parezcan políticas.

No estoy defendiendo que el Supremo tema las represalias, pues tiene una posición segura dentro del sistema constitucional estadounidense.[11] Si el Tribunal Supremo se muestra sensible a las reacciones ante sus decisiones aparentemente políticas es debido a su propia imagen de cuál es su verdadero papel. A su juicio, su papel consiste en no ser «político», sino que se concibe a sí mismo como un agente fiel que ha de limitarse a preservar los compromisos fundacionales hasta que éstos cambien.[12]

---

10 Véase, por ejemplo, John Hart Ely, *Democracy and Distrust: A Theory of Judicial Review*, Cambridge (Mass.), Harvard University Press, 1980 [ed. cast.: *Democracia y desconfianza: una teoría del control constitucional*, trad. por Magdalena Holguín, Santafé de Bogotá, Siglo del Hombre, 1997].

11 Aquí he exagerado la seguridad de la judicatura estadounidense. Un incidente con el juez de distrito Harold Baer sugiere una persistente inseguridad, especialmente en el contexto de la guerra contra las drogas. Baer dejó libre a un acusado tras desestimar un registro en el que se habían descubierto más de treinta y cinco kilogramos de narcóticos; Don Van Natta Jr., «Judge's Drug Ruling Likely to Stand», *New York Times*, 28 de enero de 1996, p. 27. La resolución fue atacada en ese momento por el candidato presidencial Robert Dole, que exigió la impugnación de Baer; Katharine Q. Seelye, «A Get Tough Message at California's Death Row», *New York Times*, 24 de marzo de 1996, p. 29. El Presidente Clinton se subió después al carro, sugiriendo que podría solicitar la renuncia de Baer si éste no revocaba su resolución; Alison Mitchell, «Clinton Pressing Judge to Relent», *New York Times*, 22 de marzo de 1996, p. 1. Ante ello Baer revocó su resolución; Don Van Natta Jr., «Under Pressure, Federal Judge Reverses Decision in Drug Case», *New York Times*, 2 de abril de 1996, p. 1. El Juez Jefe Jon Newman, del Segundo Circuito de Apelaciones, junto con otros jueces, criticó entonces los ataques de Dole contra Baer, alegando que fueron «demasiado lejos»; Don Van Natta Jr., «Judges Defend a Colleague from Attacks», *New York Times*, 29 de marzo de 1996, B1.

12 En Lessig, «Translating Federalism», *op. cit.*, describo más detalladamente la concepción que el Supremo tiene de su propio papel.

Pero cuando —como en los casos de ambigüedad latente— no hay compromisos fundacionales que preservar, cualquier tentativa de traducción parecerá ser algo más. Y siempre que parezca que el Tribunal Supremo va más allá de preservar meramente los compromisos fundacionales, se creará la percepción de que el Supremo se limita a actuar para ratificar su propia visión de un régimen constitucional adecuado, en lugar de imponer juicios cuya constitucionalidad haya sido establecida por otros.[13] En una palabra, parecerá que actúa «políticamente».

Pero ¿qué significa «político» en este contexto? No significa simplemente que el Supremo esté tomando decisiones acerca de principios o de políticas. En ningún momento se afirma que los principios constituyan razones impropias para que un tribunal decida sobre un caso. Por el contrario, las decisiones sobre principios o políticas resultan adecuadas para la aplicación de la ley siempre que sean oportunamente ratificadas por el proceso político. El problema con las decisiones en los casos de ambigüedad latente es que no parecen haber sido oportunamente ratificadas por el proceso político. Tales decisiones reflejan principios, pero éstos no parecen extraídos de la Constitución.

«Político» se refiere, pues, a juicios no ratificados claramente y discutidos en la actualidad.[14] Cuando los fundamentos mismos de un juicio se consideran básicamente impugnados, y cuando no existe razón para creer que la Constitución adopta una postura en esta disputa, entonces aplicar el resultado de una traducción concreta parecerá, en ese contexto, político.[15]

El ciberespacio va a generar una presión intensa en este sentido. Cuando un principio constitucional originario se puede traducir con cierta claridad o certeza, el Tribunal Supremo puede resistirse a las mayorías del momento en nombre de los compromisos fundacionales. Pero cuando las ambigüedades son latentes y una decisión parece realmente una decisión, la traducción no basta. Lo que defiendo aquí es que el Supremo no va a ser el lugar donde tomar tal decisión.

---

13 Robert H. Bork, *The Antitrust Paradox: A Policy at War with Itself*, Nueva York, Basic Books, 1978, p. 83.

14 Véase, por ejemplo, Felix Frankfurter, *The Commerce Clause Under Marshall, Taney, and Waite*, Chapel Hill, University of North Carolina Press, 1937, p. 82.

15 La relación entre un ámbito en disputa y un juicio político es más compleja de lo que aquí se indica. Discuto esto más extensamente en Lawrence Lessig, «Fidelity and Constraint», *Fordham Law Review*, núm. 65, 1997, p. 1365.

Puede que esta afirmación parezca demasiado pesimista, especialmente si tenemos en cuenta el éxito en la derogación de la Ley de Decencia en las Comunicaciones.[16] Pero ese caso revela en sí mismo la inestabilidad que, me temo pronto se tornará en pasividad.

A lo largo de las sentencias de los dos tribunales de primera instancia que juzgaron el caso, los tribunales se expresan como si estuvieran «hallando» hechos acerca de la naturaleza del ciberespacio. Estos «hallazgos» determinaron el resultado constitucional, y ambos tribunales presentaron sus hallazgos con una confianza que hacía que parecieran escritos sobre piedra.

Tales hallazgos eran, en su mayor parte, descripciones excepcionalmente buenas del punto en que se encontraba el ciberespacio en 1996, pero no nos contaban nada acerca de a dónde se dirigía o qué podría llegar a ser. Los tribunales se expresaban como si estuvieran informándonos de la naturaleza del ciberespacio, pero como hemos visto, éste no posee una naturaleza intrínseca. No es ni más ni menos que como se lo diseña. Al derogar los esfuerzos del Congreso para zonificar el ciberespacio, los tribunales no nos estaban diciendo lo que es el ciberespacio, sino lo que debería ser. Estaban construyendo, no hallando, la naturaleza del ciberespacio; sus decisiones son responsables, en parte, de lo que el ciberespacio llegue a ser.

Al principio no parecerá que sea así. Cuando nos enfrentamos a algo nuevo, resulta difícil discernir entre lo que es natural o viene dado y lo que es modificable. Pero con el tiempo los tribunales comprobarán que pocas cosas en el ciberespacio son «naturales». Los límites en la arquitectura del ciberespacio que se han considerado como hallazgos en una sentencia se verán más tarde como «opciones de diseño». Lo que antes era «imposible» se hará luego posible, y a medida que se produzcan estas modificaciones de lo posible, los tribunales sentirán cada vez más que no pueden pronunciarse realmente acerca de qué es el ciberespacio. Se percatarán de que sus hallazgos influyen en sus fallos, de que en parte son responsables de lo que el ciberespacio ha llegado a ser.

Esto no es más que el «principio de indeterminación» de Heisenberg aplicado al Derecho Constitucional. Y a medida que los tribunales se den cuenta, tal como han hecho en otras áreas, remitirán cada vez más estas decisiones a los poderes políticos: si estos juicios tienen un cariz político, se dejarán en manos de quienes establecen las políticas, y no de los jueces.[17]

---

16 *ACLU vs. Reno,* 929 FSupp 824, EDPa, 1996; *Shea vs. Reno,* 930 FSupp 916, SDNY, 1996.

17 Esto lo discuto en Lessig, «Fidelity and Constraint», *op. cit*.

Uno apenas puede culpar de esto a los jueces. Es más, en algunos casos deberíamos fomentar tal deferencia a las instancias políticas.[18] Ahora bien, no deberíamos subestimar sus consecuencias, pues en el futuro el poder legislativo actuará relativamente sin restricciones por parte de los tribunales; los principios que podríamos denominar constitucionales —estén o no reflejados en la Constitución estadounidense— restringirán al poder legislativo sólo si éste decide tenerlos en cuenta.

Antes de pasar a tratar qué podríamos esperar de dicho poder legislativo, consideremos otro problema relativo a los tribunales —específicamente, el problema que afronta nuestra tradición constitucional a medida que la Constitución se traslada al contexto del ciberespacio. Se trata del problema de la «acción estatal».

Las arquitecturas constituyen el ciberespacio; dichas arquitecturas son variadas y encarnan de forma diversa los principios políticos, algunos de los cuales revisten importancia constitucional. Sin embargo, en su mayor parte —y afortunadamente— estas arquitecturas son de carácter privado: se construyen en universidades o empresas y se implementan en redes que ya no están financiadas por el Departamento de Defensa. Y, al ser de carácter privado, quedan tradicionalmente fuera del alcance de la revisión constitucional. De este modo, los principios constitucionales de privacidad, acceso, derecho al anonimato e igualdad no tienen por qué perturbar este nuevo mundo, dado que es «privado» y la Constitución sólo se ocupa de la «acción estatal».

Lo que no tengo claro es por qué esto debería ser así. Si el código funciona como la ley, estamos creando la jurisdicción nueva más importante desde la compra de Louisiana,[19] pero estamos haciéndolo al margen de la revisión constitucional. Es más, estamos haciéndolo precisamente para que la Constitución no la rija —como si quisiéramos librarnos de las restricciones que imponen los principios encarnados por esa tradición.

---

18 Uno podría muy bien sostener que la deferencia del Tribunal Supremo al Congreso durante la crisis de la Gran Depresión habría resultado muy conveniente; véase, por ejemplo, Sunstein, *Democracy and the Problem of Free Speech*, *op. cit.*, p. 39.

19 El autor alude a la operación comercial por la que el Primer Imperio Francés vendió en 1803 a EEUU la Louisiana, su franja colonial en Norteamérica. Este terreno, de más de 2 millones de km^2, constituye casi una cuarta parte de la superficie actual de EEUU. El entonces Presidente Thomas Jefferson concedía una enorme importancia a la anexión de este terreno, pero se enfrentó a reticencias internas acerca de la constitucionalidad de la compra. [N. del E.]

En lo que llevo expuesto en este libro, no he confiado demasiado en esta distinción privado/público; incluso puede que el lector diga que la he ignorado.[20] Pero no la he ignorado porque carezca de sentido, sino porque no sé cómo podría ser transpuesta a la regulación del ciberespacio. El concepto mismo de acción estatal plantea una ambigüedad latente, y no creo que tengamos una idea clara de cómo resolverla.

La ambigüedad latente es ésta: la Constitución fue concebida en una época en que las arquitecturas básicas venían dadas. Sus redactores se encontraron con las leyes de la naturaleza, las de la economía y la «ley natural» de los seres humanos, ninguna de las cuales era fruto de la acción de un Estado o de las personas.

Tales arquitecturas imponían sus restricciones, por supuesto, y éstas constituían una «regulación», pero el grado hasta el cual podían usarse como herramientas de control autoconsciente era limitado. La planificación urbana no estaba limitada,[21] pero más allá de elaborar el trazado de un espacio, había poco que los padres de la Constitución pudieran hacer con respecto a las reglas que gobernarían el entorno construido de este espacio.

El ciberespacio, en cambio, posee diferentes arquitecturas cuyo poder regulador no es tan limitado. En el entorno que la gente conoce allí puede integrarse una extraordinaria cantidad de control. El tipo de información que puede recopilarse, el grado de anonimato que es posible, el acceso que se concede, la expresión que será oída —todo ello supone decisiones, no «hechos». Todo ello es diseñado, no hallado.

Nuestro contexto, por lo tanto, es muy diferente. Que el alcance de la revisión constitucional en el primer contexto fuera limitado no obliga a que sea igualmente limitado en el segundo. Podría serlo, pero no podemos darlo por sentado meramente porque fuera tan limitado en un contexto muy diferente.

Así pues, los redactores de la Constitución no nos proporcionan respuesta alguna acerca del alcance de la acción estatal. Debemos decidir por nosotros mismos qué opción encaja mejor en la tradición constitucional estadounidense. ¿Resulta más fiel a ésta permitir que estas estructuras de control,

---

20 Para la enunciación más clara de una postura contraria, véase Charles Fried, «Book Review: Perfect Freedom or Perfect Control?», *Harvard Law Review*, núm. 114, 2000, p. 606.

21 En *Albion's Seed*, *op. cit.*, Fischer muestra cómo la planificación urbana en EEUU siguió las costumbres europeas.

el equivalente funcional de la ley, se desarrollen fuera del alcance de la revisión constitucional? ¿O deberíamos extender la revisión constitucional a las estructuras de regulación privada para preservar aquellos principios fundamentales dentro de nuestra tradición?

Se trata de preguntas complejas, aunque resulta útil apuntar que no lo son tanto en otros regímenes constitucionales. La tradición alemana, por ejemplo, tendría menos problemas con la idea de que las estructuras de poder privadas deben ser confrontadas en última instancia con los principios constitucionales fundamentales.[22] La tradición alemana no es la estadounidense, por supuesto, pero el hecho de que haya respaldado esta visión sugiere que podemos hacer sitio a las restricciones de la Constitución sin convertir todo en una disputa constitucional. Es posible una decisión razonada sin convertir todo contrato privado en un caso federal.

No obstante, hará falta una revolución en el Derecho Constitucional estadounidense para que el Tribunal Supremo, al menos de forma autoconsciente, traspase los límites de la acción estatal. Algunos eruditos han esbozado cómo podría hacerse sin una remodelación radical de la legislación estadounidense, sin embargo, otros defienden que es imposible si no se reforma completamente la Constitución.[23]

En cambio, mi razón para ignorar la doctrina de la acción estatal no tiene tanto que ver con la reforma radical de la legislación cuanto con dotarnos en primer lugar de un sentido más claro sobre cómo deberíamos legislar en este nuevo espacio. Como lo expresa Paul Berman, la razón para ignorar la doctrina de la acción estatal por ahora es que:

> [...] comoquiera que se resuelvan tales cuestiones, al menos nos habrán obligado a abordar la cuestión constitucional sustantiva y a articular los principios que están en juego. La doctrina de la acción estatal, por contra, descarta por completo tales debates afirmando que la actividad en cuestión es privada

---

22 David P. Currie, *The Constitution of the Federal Republic of Germany*, Chicago, University of Chicago Press, 1994, pp. 182-187. Véase también Dawn C. Nunziato, «The Death of the Public Forum in Cyberspace», *Berkeley Technology Law Journal*, núm. 20, 2005, pp. 1115-1170, n. 2, donde describe la revisión constitucional de la legislación anti-disolución de marcas comerciales ateniéndose a la protección de la libertad de expresión consagrada en la Primera Enmienda.

23 Charles Fried, «Book Review: Perfect Freedom or Perfect Control?», *Harvard Law Review*, núm. 114, 2000, p. 606.

y que, por lo tanto, no es un asunto que competa al discurso constitucional. Si uno cree que tal discurso posee en sí mismo un valor cultural, la aplicación de la doctrina de la acción estatal conlleva un coste significativo.[24]

De nuevo, se mantiene la probabilidad de que continuemos sufriendo este coste.

Éstas son, pues, las dos formas en que los tribunales están bloqueados. Por un lado, no pueden ser creativos y, por otro, el alcance de su revisión constitucional se ha reducido (artificialmente, a mi entender) con el fin de excluir el aspecto más importante de la legislación del ciberespacio —el código. Si existen decisiones pendientes acerca de adónde deberíamos ir, así como acerca de los principios que incluirá este espacio, no podemos esperar que sean nuestros tribunales los que las tomen.

Problemas con los legisladores

Durante una conferencia en la antigua república soviética de Georgia, patrocinada por alguna agencia occidental dedicada a la democracia, un jurista irlandés estaba tratando de explicar a los georgianos lo estupendo de un sistema de «revisión judicial» (el sistema por el cual los tribunales pueden derogar las leyes promulgadas por un parlamento). «La revisión judicial», declaró entusiasta, «es maravillosa. Siempre que un tribunal deroga una ley promulgada por el Parlamento, el pueblo se pone de lado del tribunal, en contra del Parlamento. El Parlamento, cree el pueblo, se queda en lo político; el Tribunal Supremo, piensan, se funda en principios». Un amigo mío georgiano, demócrata neófito como era, preguntó: «Pero, ¿por qué en una democracia el pueblo se muestra leal a una institución no democrática y rechaza la institución democrática que hay en el sistema?». «Usted no entiende la democracia», repuso el jurista.

Cuando reflexionamos sobre la cuestión de la gobernanza en el ciberespacio —cuando pensamos en las decisiones que he bosquejado, especialmente en aquéllas surgidas en la Tercera Parte—, es probable que experimentemos

24 Paul Schiff Berman, «Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation», *University of Colorado Law Review*, núm. 71, 2000, pp. 1263-1269.

una sensación de abatimiento. Parece casi imposible concebir esta idea de gobernar el ciberespacio. ¿Quién es el ciberespacio? ¿Dónde tendría que votar? La mera idea parece repeler al propio ciberespacio.

Sin embargo, nuestro problema aquí no tiene que ver con la gobernanza en el ciberespacio, sino con la gobernanza en sí misma. El ciberespacio no plantea un conjunto especial de dilemas, sino sólo los dilemas conocidos de la gobernanza moderna, pero situados en un nuevo lugar. Algunos aspectos son diferentes, como sus objetivos o el alcance de los intereses internacionales, pero la dificultad no provendrá del objetivo distinto sino de nuestro problema con la gobernanza.

A lo largo de este libro me he afanado en identificar las decisiones que nos plantea el ciberespacio. He sostenido que su misma arquitectura está a disposición de quien la quiera modificar, y que, dependiendo de quien lo haga, podrían darse varios resultados diferentes. Algunas de esas decisiones son claramente de carácter colectivo —son decisiones acerca de cómo vivir colectivamente en este espacio. Uno habría pensado que las decisiones colectivas eran problemas de gobernanza, pero muy pocos de nosotros desearíamos que fuera el Estado el que las tomara. El Estado no parece ser la solución a ninguno de nuestros problemas, y deberíamos comprender por qué esto es así. Deberíamos comprender al jurista irlandés que todos llevamos dentro.

Nuestro escepticismo no es una cuestión de principios. La mayoría de nosotros no somos liberales [*libertarians*]; puede que seamos contrarios al Estado, pero en la mayor parte de las ocasiones creemos que existen principios colectivos que deberían regular la acción privada («colectivos» en el sentido estricto de que todos los individuos actuando por su cuenta promoverán menos esos principios que si dicha acción individual pudiera coordinarse). También estamos comprometidos con la idea de que los principios colectivos deberían regular el emergente mundo técnico. Nuestro problema es que no sabemos cómo debería ser regulado este mundo, ni por quién. Y tememos que los principios que se adopten no sean los correctos.

Al igual que el jurista irlandés, estamos hartos de los Estados y nos mostramos profundamente escépticos acerca del producto de la política democrática. Estamos convencidos, acertadamente o no, de que estos procesos han sido capturados por intereses especiales más preocupados por los principios individuales que por los colectivos. Aunque creemos que existe un papel reservado a los juicios colectivos, nos repulsa la idea de poner el diseño de algo tan importante como Internet en manos de los Estados.

Abundan los ejemplos de esto, y la pauta resulta llamativa. El único mensaje del Estado en su descripción de cuál debería ser su papel en el ciberespacio es que simplemente debería quedarse al margen. En el ámbito del comercio electrónico, el Estado afirma que dicho comercio debería cuidarse por sí mismo. Por supuesto, al mismo tiempo aprueba toda suerte de leyes para incrementar las protecciones de la propiedad intelectual, mostrándose también aparentemente entusiasmado con la regulación del contenido «indecente» sin importar el pujante comercio que representa.

Un ejemplo perfecto de esto es la cesión estatal del control de la gestión del sistema de nombres de dominio. Durante algún tiempo el Estado había estado reflexionando sobre la mejor forma de continuar el gobierno o el control de dicho sistema.[25] Originariamente había delegado la tarea mediante contratos realizados por la NSF (*National Science Foundation*, Fundación Nacional de la Ciencia), primero con una organización californiana sin ánimo de lucro dirigida por el difunto Jon Postel, y después con una empresa privada llamada Network Solutions.

Sin embargo, estaba previsto que dichos contratos vencieran en 1998, y durante un año el Estado consideró seriamente lo que debía hacer. En junio de 1998 publicó un Libro Blanco donde apelaba al establecimiento de una organización sin ánimo de lucro consagrada al interés colectivo de Internet en su conjunto y encargada de decidir las políticas relativas al gobierno del sistema de nombres de dominio. Se le iba a quitar al Estado el poder para establecer políticas en Internet, poniéndolo en manos de una organización fuera de su control. En 1998 se llevó a cabo tal traspaso de poderes mediante la creación de la ICANN (*Internet Corporation for Assigned Names and Numbers*, Corporación de Internet para la Asignación de Nombres y Números), que, según su página web está:

> Dedicada a preservar la estabilidad operativa de Internet, a promover la competencia, a lograr una amplia representación de las comunidades mundiales de Internet, y a desarrollar políticas adecuadas a su misión a través de procesos de abajo a arriba basados en el consenso. ICANN, una entidad pública benéfica sin ánimo de lucro, es la organización internacional responsable de la gestión y supervisión de la coordinación del sistema de nombres de dominio de Internet y de sus identificadores únicos.[26]

---

25 A. Michael Froomkin, «The Collision of Trademarks, Domain Names, and Due Process in Cyberspace», *Communications of the ACM*, núm. 44, 2001, p. 91. Véase también Jonathan Weinberg, «ICANN and the Problem of Legitimacy», *Duke Law Journal*, núm. 50, 2000, p. 187.

26 Internet Corporation for Assigned Names and Numbers, disponible en http://icann.org/index.html.

Pensemos en el tipo de preguntas que le surgirían a mi amigo georgiano acerca de esta maniobra. ¿Una «corporación sin ánimo de lucro dedicada al interés colectivo»? ¿No es precisamente eso lo que se supone que es un Estado? ¿Un consejo compuesto de grupos de interés representativos? ¿No es eso lo que es un Congreso? Es más, puede que mi amigo georgiano observe que esta estructura corporativa difiere del Estado en un único aspecto destacado —no existe ningún requisito de elecciones.

Se trata de conferir la elaboración de políticas a lo que es en efecto una agencia independiente, pero una completamente al margen del proceso democrático. ¿Qué dice esto de nosotros? ¿Qué significado tiene que nuestro instinto natural sea delegar el poder de elaborar las políticas en organismos al margen del proceso democrático?

En primer lugar, esto refleja la patética resignación que la mayoría de nosotros siente acerca de los resultados del gobierno ordinario. Hemos perdido la fe en la idea de que la obra del gobierno representativo pueda representar algo más que meros intereses —de que, apropiándome de la frase inicial de la última sentencia al frente del Tribunal Supremo del juez Marshall, el poder, y no la razón, es ahora la moneda corriente de la democracia deliberativa.[27] Hemos abandonado la idea de que el gobierno ordinario puede funcionar, y tan profunda es la desesperación que ni siquiera el propio Estado cree que deba desempeñar un papel en la regulación del ciberespacio.

Yo comprendo esta resignación, pero es algo que hemos de superar. Debemos aislar sus causas y separarlas de sus efectos. Si odiamos al Estado, no es porque la idea de los principios colectivos constituya un anatema para nosotros, sino porque hemos crecido cansados de nuestro Estado, hastiados de sus traiciones, de sus juegos y de los intereses que lo controlan. No obstante, debemos hallar la forma de superar tal hastío.

Una causa central de la disfunción gubernamental es la corrupción sugerida por el modo en que se elige al gobierno. No me refiero a «corrupción» en el sentido tradicional, la corrupción que mina la energía de tantas naciones en desarrollo. No creo que los congresistas acepten sobornos (el congresista de California Randy Cunningham constituye una excepción, por supuesto),[28]

27 *Payne vs. Tennessee*, 501 U.S. 808, 844, 1991 (Marshall, voto particular).

28 Véase Wikipedia, «Duke Cunningham», disponible en: http://en.wikipedia.org/wiki/Randy_%22Duke%22_Cunningham.

ni que sus motivaciones sean impuras. Ellos tratan de hacerlo lo mejor que pueden en el mundo donde habitan; es ese mundo el que supone el problema.

Y es que en ese mundo el dinero controla la atención. Para llegar a ser miembro de la Cámara de Representantes, hay que presentar una candidatura. En 2004 si alguien se presentaba candidato en un distrito abierto, gastaba una media de 1.086.437 dólares; si llegaba a ganar, gastaba 1.442.216 dólares. Ese mismo año si alguien se presentaba contra un candidato a la reelección, tenía un 97,5 % de posibilidades de no ganar (sólo ocho aspirantes lo consiguieron). En las elecciones al Senado de 2004, sólo un aspirante logró desbancar a un candidato a la reelección. En EEUU, por lo tanto, el ejercicio de un cargo político conlleva la permanencia vitalicia en él, hasta tal punto que el periodo medio de mandato de un congresista rivaliza con el de un juez del Tribunal Supremo.[29]

Para recaudar tal cantidad de dinero, los miembros del Congreso deben dedicar su tiempo a hacer felices a los ricos, lo cual pasa por escuchar sus problemas y, a veces, por impulsar leyes que los resuelvan. Esto suena bastante inofensivo hasta que caemos en la cuenta de cuánto tiempo consagran a esta recaudación de fondos. El ex senador Hollings calculaba que un senador dedica a esta tarea la tercera parte de su tiempo,[30] lo cual probablemente sea una importante subestimación.[31]

Ahora recapacitemos acerca de cuán absurdas son estas prioridades. Al fin y al cabo, los congresistas trabajan para nosotros. Si una empleada de restaurante se pasase la tercera parte de su jornada laboral organizándose para ir a trabajar, la despedirían. Sin embargo, eso es esencialmente lo que sucede en Washington. La fracción de tiempo más importante de los miembros del Congreso es la dedicada a recaudar dinero para seguir siendo miembros del Congreso. ¿Es realmente para esto para lo que les pagamos?

---

29 El periodo medio de mandato de un juez del Tribunal Supremo es de 15 años, mientras que el de los senadores que ostentaban su cargo entre enero de 2005 y enero de 2007 era de 12,1 años, y de 9,3 años el de los miembros de la Cámara de Representantes. Véase http://www.supremecourtus.gov/about/institution.pdf. Las cifras de los gastos de campaña se extraen de http://www.senate.gov/reference/resources/pdf/RS22007.pdf.

30 Ernest F. Hollings, «Stop the Money Chase», Washington Post, Página B07, 19 de febrero de 2006, disponible en http://www.washingtonpost.com/wp-dyn/content/article/2006/02/17/AR2006021701847.html.

31 Las cifras de Hollings se confirman en Peter Francia y Paul Herrnson, «The Impact of Public Finance Laws on Fundraising in State Legislative Elections», *American Politics Research*, vol. 31, núm. 5, septiembre de 2003.

Aquí el problema no es tanto que los miembros del Congreso no estén haciendo su trabajo, sino el modo en que dicho trabajo queda desvirtuado por esta necesidad de recaudar dinero. Los objetivos más fáciles para recaudar fondos son los grupos de presión, y éstos están rebosantes de ideas sobre cómo amoldar la legislación a su propio beneficio.

Y así el Congreso se amolda, y la legislación se modifica para beneficiar a los más poderosos económicamente. No se trata tanto de capitalismo como de dominio de los grupos de presión. Nuestra economía se define por una combinación de leyes y poder que beneficia sólo a algunos.

Para quebrar este dominio de los grupos de presión, se necesita una manera de llamar la atención de los miembros del Congreso. Pero hasta que el sistema no cambie, la única manera de llamar su atención es mediante dinero. He aquí el círculo de resultados viciosos para la democracia. El Congreso sólo ve lo que un reducido grupo quiere que vean, y ello a menudo no tiene ninguna conexión evidente con la verdad.

Si hay decisiones pendientes acerca de cómo crecerá el ciberespacio, entonces tales decisiones se tomarán. La única pregunta es quién lo hará. Podemos quedarnos de brazos cruzados y no hacer nada mientras otros —los que no se limitan a quedarse de brazos cruzados— toman estas decisiones, o podemos tratar de imaginar un mundo donde de nuevo puedan tomarse las decisiones de manera colectiva y responsable.

Problemas con el código

Durante un taller celebrado en la Universidad de Harvard poco antes de la aparición de la primera edición de este libro, Jean Camp, una ingeniera informática que impartía clases en la Escuela de Gobierno Kennedy de la misma universidad, afirmó que yo había errado en mi planteamiento. El problema, aseguró, no es que «el código sea la ley» o que «el código regule», sino que «no hemos tenido una conversación sobre cómo regula el código». Y dirigiéndose a continuación al resto del auditorio, preguntó: «¿Les gustó a todos ustedes el debate que tuvimos sobre si los documentos de Microsoft Word deberían llevar un número de identificación único? ¿Les resultó satisfactorio?».

Su ironía comportaba una idea importante, así como un error interesante. Por supuesto, para una informática el código es la ley. Y si el código es la ley, entonces la pregunta que deberíamos plantear es obviamente ésta: ¿quiénes son los

legisladores? ¿Quién redacta esta ley que nos regula? ¿Qué papel desempeñamos nosotros en la definición de esta regulación? ¿Qué derecho tenemos a saber de ella? Y, por último, ¿cómo podríamos intervenir para controlarla?

Todo esto resulta perfectamente obvio para alguien que piensa y respira las regulaciones del código. Pero para un abogado, como Camp o como yo, a lo largo de este libro, hemos cometido un error muy básico. El código no es la ley, como tampoco lo es el diseño de un avión; el código no regula, como tampoco lo hacen los edificios; el código no es público, como tampoco lo es una cadena de televisión. Poder debatir y decidir es una oportunidad que exigimos con respecto a la regulación pública, no a la acción privada.

El error de Camp es muy bueno. Se trata de un error que deberíamos cometer más gente más a menudo. Porque aunque el código sea por supuesto privado, y por supuesto diferente de los códigos legales de EEUU, sus diferencias no implican que no existan también similitudes. «El código de la Costa Este» —la ley— regula posibilitando y limitando las opciones que tienen los individuos, con el fin de persuadirlos para comportarse de una determinada manera. «El código de la Costa Oeste» hace lo mismo. El código de la Costa Este regula incrementando los costes a los que se enfrentan quienes se desvíen de las reglas requeridas por el código. El código de la Costa Oeste hace lo mismo. Y aunque podríamos sostener que el Código de Costa Este es más común —que regula y controla una parte mucho mayor de nuestras vidas—, ésa es una diferencia de grado, no cualitativa. Se trata de una razón que hemos de sopesar, una razón para no mantenernos indiferentes ante el código.

Por supuesto, existen diferencias entre la ley y el código. No creo que todo sea necesariamente público, o que la Constitución debiera regular todos los aspectos de la vida privada. Cuando apago la radio para no oír a Rush Limbaugh, no creo que se trate de una cuestión constitucional. Sin embargo, afirmar que debería haber una diferencia no equivale a afirmar que la diferencia deba ser tan absoluta como la plantea el actual pensamiento constitucional. Cuando los juristas decimos a las Jean Camps del mundo que simplemente están cometiendo un «error» al trasladar los principios del Derecho Público al código, somos más bien nosotros quienes estamos cometiéndolo. La cuestión de si el código debería confrontarse con estas restricciones de los principios públicos constituye una pregunta, no una conclusión, y ha de decidirse por medio de discusión, no de definición.

Esto no será fácil, desde luego. El código es técnico y los tribunales no están bien posicionados para evaluar tales detalles técnicos. Pero incluso así, el fracaso consiste en no intentarlo siquiera. El formalismo del

Derecho estadounidense, que coloca más allá de la revisión constitucional estas estructuras de control, constituye una tercera patología que inhibe la elección. Los tribunales están maniatados, los legisladores son patéticos y el código es intocable. He aquí nuestra condición actual, una combinación que resulta mortífera para la acción —una combinación que garantiza que se va a hacer poco.

17. Respuestas

NECESITAMOS UN PLAN. Hasta ahora he contado una lóbrega historia sobre las decisiones que plantea el ciberespacio, y sobre nuestra incapacidad para afrontarlas. He vinculado esta incapacidad a tres características de nuestra actual cultura legal y política. En este breve capítulo, considero tres respuestas. Estas respuestas no son más que bosquejos, pero deberían bastar para sugerir la naturaleza de los cambios que hemos de llevar a cabo.

Respuestas del poder judicial

Previamente he afirmado que deberíamos interpretar la vacilación judicial como algo basado en la prudencia. Cuando existen tantas opciones posibles y no hay una regla claramente establecida, a un tribunal le resulta difícil aparecer como tal al tiempo que decide qué políticas pueden ser mejores.[1]

Aunque, en general, estoy de acuerdo con este ideal de prudencia, creo que tenemos que darle unas vueltas —para contextualizarlo y limitar su alcance. Deberíamos identificar el origen de las dificultades de los jueces. A veces, cierta vacilación antes de resolver las cuestiones relacionadas con la Constitución en el ciberespacio de manera definitiva —firme o con alguna pretensión de permanencia— resulta totalmente adecuada.

---

1 Deborah Hellman, en «The Importance of Appearing Principled», *Arizona Law Review*, núm. 37, 1995, p. 1107, describe los costes de legitimidad en que incurren los tribunales cuando anulan precedentes por razones aparentemente políticas.

En otros casos, sin embargo, los jueces —especialmente los de tribunales de primera instancia— deberían mostrarse más seguros, ya que son muchos, y muchos de ellos son extraordinariamente talentosos y creativos. Sus voces podrían enseñarnos algo respecto a este ámbito, aunque sus fallos fueran provisionales o limitados en su alcance.

En los casos de simple traducción (donde no hay ambigüedades latentes y la tradición constitucional parece hablar claramente), los jueces deberían proponer firmemente argumentos que traten de preservar los principios originales de la libertad en un nuevo contexto. En estos casos hay un importante espacio para el activismo. Los jueces deberían identificar nuestros principios y defenderlos, no necesariamente porque sean correctos, sino porque la única razón para ignorarlos es que hayan sido rechazados —no por un tribunal, sino por el pueblo.

En los casos donde la traducción no es tan sencilla (los casos que plantean ambigüedades latentes), los jueces, especialmente aquéllos de los tribunales de primera instancia, desempeñan un papel diferente. En estos casos los jueces deberían quejarse constantemente. Deberían comentar las cuestiones que estos cambios suscitan e identificar los principios que están en liza. Incluso si la decisión que deben adoptar en un caso concreto es comedida o pasiva, debería ser comedida en señal de protesta. Es muy posible que estos casos apelen a la prudencia, pero para justificar su pasividad y compensar por dejar que reivindicaciones de derechos caigan en saco roto, los jueces deberían plantear, ante la cultura legal, el conflicto que dichas reivindicaciones presentan. Los casos difíciles no tienen que dar lugar a mala legislación, pero tampoco deberían ser tratados como si fueran fáciles.

Ésta es la respuesta más simple al problema de la ambigüedad latente, pero es incompleta. Nos obliga a enfrentarnos a cuestiones de principios constitucionales y a elegir, pero una solución mejor nos ayudaría a resolverlas. A pesar de que la tarea de los tribunales nunca será tomar decisiones definitivas sobre cuestiones de principios, al suscitar tales cuestiones los tribunales pueden inspirar a otros a decidir sobre ellas.

Ésta es la idea que hay detrás de la doctrina de la revisión esbozada hace veinte años por Guido Calabresi, profesor universitario por entonces y actualmente juez.[2] Extremadamente simplificada, la idea es la siguiente:

---

2 Guido Calabresi, A Common Law for the Age of Statutes, Cambridge (Mass.), Harvard University Press, 1982, pp. 16-32; Guido Calabresi, «The Supreme Court, 1990 Term-Foreword: Antidiscrimination and Constitutional Accountability (What the Bork-Brennan Debate Ignores)», Harvard Law Review, núm. 105, 1991, pp. 80, 83, 103-107, 119-120.

cuando el Tribunal Supremo se enfrenta a asuntos que se presentan abiertos, pero que constituyen cuestiones fundamentales de principios, debería afrontar el conflicto de manera abierta y reconocer que la Constitución no lo resuelve claramente. No obstante, el Supremo tendría que proceder a resolverlo de la forma que con más probabilidad suponga la revisión democrática de la resolución. Si la resolución promueve la revisión adecuada, el Supremo podría hacer prevalecer sus resultados. A lo máximo que debería llegar el Supremo en estos casos es a asegurar que la democracia tiene su voz; su tarea no consiste en sustituir los puntos de vista democráticos por sus principios.

Muchos ridiculizan esta solución,[3] afirmando que los redactores de la Constitución claramente no tenían en mente nada de esto cuando crearon el Tribunal Supremo y permitieron la revisión judicial. Por supuesto que no. La doctrina de la revisión no está diseñada para los problemas que los redactores tenían en mente. Por lo tanto, como respuesta a los problemas de las ambigüedades latentes, ella misma revela una ambigüedad latente.

Podríamos negar esta ambigüedad. Podríamos afirmar que los redactores previeron que el Tribunal Supremo no haría absolutamente nada con respecto a las ambigüedades latentes; que, en tales contextos, el proceso democrático intervendría, mediante el Artículo V, para corregir una aplicación incorrecta o para responder a un cambio de circunstancias. Es muy posible que éste fuera su punto de vista. Sin embargo, no creo que tal intención esté lo bastante clara como para excluir de antemano nuestra consideración acerca de cómo podríamos afrontar mejor las próximas series de cuestiones sobre la aplicación de los principios constitucionales al ciberespacio. Prefiero pecar de activismo inofensivo que de pasividad debilitante. Se trata de un papel mínimo que los tribunales han de desempeñar dentro de la discusión mucho más amplia que necesitamos mantener —pero que hasta la fecha no ha comenzado.

---

[3] O se quedan muy cerca de hacerlo; véase Richard A. Posner, *The Problems of Jurisprudence*, Cambridge (Mass.), Harvard University Press, 1990, pp. 300-301.

Respuestas para el código

Un segundo reto consiste en afrontar la ley que hay en el código —es decir, resolver el modo en que pensamos acerca del poder regulador del código. Hay una serie de ideas que, en conjunto, nos empujarían a un mundo donde la regulación impuesta a través de código tendría que satisfacer las normas constitucionales.

Aquí aparece de nuevo el vínculo con el código abierto. Cuando en el Capítulo 8 describí un tipo de mecanismo de control que impondría el código abierto sobre la regulación estatal, afirmé que al Estado le costaría más ocultar su regulación con el código abierto, y que a quienes lo adoptaran les resultaría más fácil desactivar cualquier regulación estatal. El paso del código cerrado al código abierto suponía un paso hacia una menor regulabilidad. A menos que estemos entregados simplemente a desactivar el poder del Estado, este paso no puede ser inequívocamente bueno.

Y es que la restricción que podría imponer el código abierto consta de dos partes; una es ciertamente buena y la otra no es necesariamente terrible. La primera parte es la transparencia —las regulaciones serían conocidas; la segunda es la resistencia —conociéndolas, se podría resistir más fácilmente a ellas. La segunda parte no tiene por qué derivarse de la primera, y no tiene por qué ser debilitante. Puede que sea más fácil desactivar las regulaciones del código si éste es abierto, pero si la regulación es legítima, el Estado puede exigir que no se desactive. Y si quiere, puede castigar a quienes la desobedezcan.

Comparemos esto con la regulación de los cinturones de seguridad. Durante un tiempo el gobierno federal estadounidense exigió que los automóviles nuevos estuviesen equipados con cinturones de seguridad automáticos. Se trataba de una regulación del código —los automóviles serían más seguros mediante una regulación del código que obligara a la gente a usar los cinturones de seguridad. Mucha gente odiaba los cinturones de seguridad, y algunos los inutilizaban, pero la virtud de esta regulación radicaba en su transparencia. Nadie albergaba dudas sobre quién era responsable de la regla que imponía el cinturón de seguridad. Si al gobierno no le gustaba que la gente inutilizara sus cinturones, era libre de aprobar leyes para castigar dicha conducta. Finalmente el gobierno no presionó más allá en este sentido —no porque no pudiera, sino porque los costes políticos habrían sido demasiado altos. La política funcionó como mecanismo de control de la regulación gubernamental, tal y como debería ser.

Esto es lo máximo que podemos esperar de la regulación del código en el ciberespacio. Existe una compensación entre la transparencia y la efectividad. La regulación del código en el contexto del código abierto es más transparente, pero también menos vinculante. El poder estatal para lograr sus fines reguladores quedaría así limitado por el código abierto.

Pero hay otro beneficio. El código cerrado facilitaría al Estado ocultar su regulación y, por ende, lograr un fin regulador ilícito. En consecuencia, con el código abierto no se da una simple derrota del Estado, sino una compensación —entre publicidad y poder, entre la transparencia de las reglas y la obediencia del pueblo. Constituye un importante mecanismo de control sobre el poder estatal declarar que las únicas normas que el Estado puede imponer son aquéllas que serían obedecidas si se impusieran de manera transparente.

¿Significa esto que deberíamos impulsar el código abierto en lugar del cerrado? ¿Significa que deberíamos prohibir el código cerrado?

No. De estas observaciones no se desprende que debamos prohibir el código cerrado o tener un mundo donde sólo exista el código abierto. Sin embargo, dichas observaciones sí apuntan hacia los principios sobre los que deberíamos hacer hincapié para todo código que regule. Si el código se erige en legislador, entonces debería abrazar los principios de los procesos legislativos.

El núcleo de estos principios es la transparencia. Lo que hace una regulación mediante código debería ser al menos tan evidente como lo que hace una regulación legal. El código abierto proporcionaría tal transparencia —no para todos (no todo el mundo lee el código), y no de manera perfecta (el código mal escrito oculta bien sus funciones), pero sí de manera más completa que el código cerrado.

Cierto código cerrado podría proporcionar esta transparencia. Si el código fuera más modular —si un escritor de código tomara simplemente componentes de un estante para incorporarlos a su sistema, como quien compra bujías para un coche—, entonces, aunque el código de tales componentes fuese cerrado, las funciones y la regulación del producto final serían abiertas.[4] La arquitectura basada en componentes podría ser tan transparente como la arquitectura de código abierto, con lo cual podría lograrse la transparencia sin necesidad de desvelar el código.

---

4 Estoy agradecido a Viktor Mayer-Schoenberger por demostrarme este planteamiento. Hal Abelson señala que los componentes tendrían que ser verificables en caso de no ser ellos mismos abiertos. De lo contrario, los componentes podrían funcionar como Caballos de Troya —fingiendo ser una cosa cuando en realidad son otra.

El mejor código (desde la perspectiva de los principios constitucionales) es tanto modular como abierto. Que sea modular asegura que los peores componentes podrían sustituirse por otros mejores. Y desde una perspectiva competitiva, ello también permite una mayor competencia en el desarrollo de mejoras dentro de un proyecto codificador concreto.

Resulta verosímil, no obstante, que determinados fragmentos de código no puedan producirse como código abierto, esto es, que el código cerrado sea a veces necesario para la supervivencia competitiva. En ese caso, el compromiso de un sistema basado en componentes del sistema permitiría conseguir algo de lo mejor de ambos mundos —algunas ventajas competitivas junto con la transparencia en su funcionamiento.

Así pues, he argumentado a favor del código transparente por los principios constitucionales que encarna, y no en contra del código como regulador o en contra de la regulación. Lo que he defendido es que insistamos en la transparencia de la regulación y que impulsemos estructuras codificadoras que incrementen tal transparencia.

La ley actualmente no lo hace. Es más, como sostienen Mark Lemley y David O'Brien, la estructura existente de protección de copyright en el ámbito del software tiende a impulsar el desarrollo de software alejado de la estructura modular.[5] La ley prefiere el código opaco al transparente, y construye incentivos para ocultar el código en lugar de para hacer evidente su funcionalidad.

Muchos han defendido que los actuales incentivos legales son ineficaces —que tienden a reducir la competencia en la producción de software.[6] Es muy posible que sea cierto, pero la mayor perversidad es nuevamente constitucional. Nuestra ley crea un incentivo para cercar todo el procomún intelectual que sea posible, impide la publicidad y la transparencia y contribuye a producir, de hecho, un Estado enormemente secreto.

---

5 Véase Mark A. Lemley y David W. O'Brien, «Encouraging Software Reuse», *Stanford Law Review*, núm. 49, 1997, p. 255. Véase también, por ejemplo, James Boyle, «A Politics of Intellectual Property: Environmentalism for the Net», disponible en http://www.law.duke.edu/boylesite/intprop.htm.

6 Para un extraordinario informe sobre los perjuicios que la Ley de copyright ha ocasionado al desarrollo de software, véase Mark Haynes, «Black Holes of Innovation in the Software Arts», *Berkeley Technology Law Journal*, núm. 14, 1999, p. 503. Véase también David McGowan, «Legal Implications of Open Source Software», *Illinois University Law Review*, núm. 241, 2001.

He aquí un ámbito en el que realizar cambios jurídicos concretos. Sin resolver la disyuntiva de si es mejor el código cerrado o el abierto, al menos podríamos impulsar el código cerrado en una dirección que facilitara una mayor transparencia. Pero la inercia de la legislación vigente —que concede a los fabricantes de software plazos de protección ilimitados en la práctica— actúa en contra de este cambio. Simplemente, la política está ausente.

Respuestas de una democracia

En su merecidamente famoso libro *Profiles in Courage*, el entonces senador John F. Kennedy relata la historia de Daniel Webster, quien, en mitad de una batalla en torno a un pacto que pensaba que dividiría la nación, afirmó en el Senado: «Señor Presidente, hoy deseo hablar no como ciudadano de Massachusetts, ni como ciudadano del Norte, sino como estadounidense».[7]

Cuando Webster pronunció esta frase —en 1850—, las palabras «no como ciudadano de Massachusetts» tenían un significado que probablemente se nos escape en la actualidad. Para nosotros, la declaración de Webster parece perfectamente normal. ¿Qué otra cosa podría ser sino estadounidense? ¿De qué otra manera podría hablar?

Ahora bien, estas palabras se pronunciaron en la cúspide de una nueva época en EEUU. Llegaron justo en el momento en que la atención de los ciudadanos estadounidenses se estaba desplazando de su condición de ciudadanos de un Estado a su condición de ciudadanos de la nación en su conjunto. Webster habló precisamente en el momento en que comenzaba a ser posible identificarse como miembro de una nación, además de como miembro de un Estado.

Como ya he explicado, en el momento de la fundación, los ciudadanos de EEUU (un concepto controvertido en sí mismo) eran en primer lugar ciudadanos de Estados particulares. Eran leales a sus respectivos Estados porque sus vidas se veían determinadas por el lugar donde vivían. Los demás Estados les resultaban tan remotos como el Tíbet nos resulta a nosotros —es más, hoy para nosotros es más fácil viajar al Tíbet de lo que era para un ciudadano de Carolina del Sur visitar el Estado de Maine.

---

7 Kennedy, *Profiles in Courage*, *op. cit.*, p. 71.

Con el paso del tiempo, por supuesto, esta situación cambió. Durante la lucha que desembocó en la Guerra Civil, las batallas de la Reconstrucción y la Revolución Industrial que vino después, la identificación de los ciudadanos con su condición de estadounidenses creció. A través de aquellos intercambios y batallas, nació una identidad nacional. Sólo en el momento en que los ciudadanos se vincularon con ciudadanos de otros Estados se pudo crear una nación.

Es fácil olvidar estos momentos de transformación, y aún más fácil imaginar que sólo ocurren en tiempos pasados. Sin embargo, nadie puede negar que el sentido de ser «estadounidense» se transformó en el siglo XIX, del mismo modo que nadie puede negar que el sentido de ser «europeo» está transformándose en la Europa actual. Las naciones se construyen a medida que la gente se percibe a sí misma como perteneciente a una cultura política común. Y tal transformación sigue en marcha para nosotros en la actualidad.

Hoy en día nos encontramos a pocos años de la situación en que se encontraba Webster en 1850. Nos encontramos a punto de poder afirmar «Hablo como ciudadano del mundo» sin que el ciudadano de a pie piense «Menudo chiflado». Estamos justo en la cúspide de una época en la que los ciudadanos comenzarán a sentir los efectos de las regulaciones de otros Estados, al igual que los ciudadanos de Massachusetts llegaron a sentir los efectos de la esclavitud y los ciudadanos de Virginia llegaron a sentir los efectos de una campaña por la libertad. Como afirma Nicholas Negroponte: «Hoy las naciones tienen un tamaño equivocado. No son lo bastante pequeñas para ser locales ni lo bastante grandes para ser mundiales».[8] Y esta inadaptación reviste importancia.

A medida que los ciudadanos de EEUU invirtamos más tiempo y dinero en este espacio que no forma parte de ninguna jurisdicción concreta, sino que está sujeto a las regulaciones de todas las jurisdicciones, nos plantearemos cada vez más preguntas acerca de nuestro estatus en él. Comenzaremos a sentir el derecho que Webster sintió, en calidad de estadounidense, a opinar sobre la vida en otras partes de EEUU. En nuestro caso se tratará del derecho a hablar sobre la vida en otras partes del mundo, fundamentado en la sensación de que existe una comunidad de intereses que va más allá de los vínculos diplomáticos y que alcanza los corazones de los ciudadanos de a pie.

---

8 Véase Nicholas Negroponte, *Being Digital*, Nueva York, Alfred A. Knopf, 1995, pp. 18, 238 [ed. cast.: *El mundo digital*, trad. por Marisa Aboala, Barcelona, Ediciones B, 1999].

¿Qué haremos entonces? ¿Qué haremos cuando sintamos que formamos parte de un mundo, y que ese mundo nos regula? ¿Qué haremos cuando necesitemos tomar decisiones sobre la forma en que ese mundo nos regula, y sobre la forma en que nosotros lo regulamos?

El hartazgo respecto al Estado que describí al final del Capítulo 16 no es una condición carente de causa. Ahora bien, su causa no supone la muerte de todo ideal de democracia. Todos nosotros seguimos siendo demócratas; la cuestión es simplemente que no nos gusta lo que nuestra democracia ha producido, y nos cuesta imaginar la extensión de lo que tenemos a nuevos dominios como el ciberespacio. Para encontrar allí más de lo mismo —más excesos y traiciones estatales como las que hemos conocido—, entonces mejor que haya menos.

Nos encontramos aquí con dos problemas, aunque sólo uno de ellos está realmente vinculado al argumento de este libro, por lo que éste será el único que discutiré en profundidad. El otro ya lo mencioné al final del Capítulo 16 —la corrupción básica de cualquier sistema que permite arrogarse tanta influencia política a quienes reparten dinero. Se trata de la corrupción que hay detrás de la financiación de las campañas electorales, una corrupción no achacable a la gente, sino al propio proceso político. Incluso a las almas cándidas del Congreso no les queda otra opción que emplear una parte cada vez mayor de su tiempo en recaudar una cantidad cada vez mayor de dinero para poder competir en las elecciones. Estamos ante una carrera armamentística, y el Tribunal Supremo ha ratificado que la Constitución así exige que sea. Hasta que no se resuelva este problema, tengo poca fe en lo que vaya a producir nuestra democracia.

La solución a este problema es evidente, por más que los detalles resulten extremadamente complicados: invertir recursos públicos en financiar campañas públicas. El coste total de las elecciones federales de 2004 rondó probablemente los 400 millones de dólares.[9] En el mismo año, EEUU gastó 38.400 millones en defensa y 660.000 millones en la guerra de Irak.[10] Independientemente de lo que el lector piense acerca de la sensatez de los gastos de defensa y de la guerra de Irak, al menos el propósito de las tres partidas es el mismo —preservar y promover la democracia. ¿Hay alguna

---

9 Center for Responsive Politics, «2004 Elections Expected to Cost Nearly $4 Billion», 21 de octubre de 2004, disponible en http://www.opensecrets.org/pressreleases/2004/04spending.asp.

10 Chris Edwards, «Bush's Overspending Problem», CATO Institute, 6 de febrero de 2003, disponible en http://www.cato.org/research/articles/edwards-030206.html.

duda de que si convirtiéramos en irrelevantes para la política las contribuciones a las campañas, lograríamos un efecto más seguro y positivo sobre la democracia que con los otros dos gastos?

Pero hay una segunda razón, extrañamente contraria a la intuición, que explica este creciente fracaso de la democracia. No es que las autoridades escuchen demasiado poco las opiniones del pueblo, es que las escuchan demasiado. Cada capricho de la población queda amplificado en los sondeos, y éstos a su vez marcan el pulso democrático. Ahora bien, el mensaje que transmiten los sondeos no es el mensaje de la democracia; su frecuencia e influencia no son producto de su creciente importancia. Si el Presidente guía sus políticas basándose en sondeos aparecidos de la noche a la mañana, es simplemente porque realizarlos resulta muy sencillo.

Se trata de un problema parcialmente tecnológico. Los sondeos marcan una interacción entre tecnología y democracia que sólo ahora estamos empezando a vislumbrar. A medida que se reduce el coste del seguimiento de la opinión instantánea de la población, y que se construyen máquinas para su supervisión permanente, producimos un flujo perpetuo de información referente a lo que «el pueblo» piensa acerca de todas las cuestiones que las autoridades puedan considerar.

Un cierto tipo de código perfecciona la maquinaria de seguimiento —un código que automatiza la selección perfecta de la muestra, que facilita bases de datos con los resultados y que simplifica el proceso de conexión. Rara vez nos preguntamos, sin embargo, si la supervisión perfecta es algo bueno.

Nuestro ideal nunca ha sido —al menos constitucionalmente— que la democracia fuese un reflejo perfecto de la «temperatura» actual del pueblo. Los redactores de la Constitución se aplicaron en diseñar estructuras que mediaran las opiniones del pueblo. La democracia había de ser algo más que una retahíla de pronunciamentos agitados; tenía que ser deliberativa, reflexiva y equilibrada por medio de las limitaciones impuestas por una constitución.

Pero quizás, para ser coherente con los argumentos expuestos en la Tercera Parte, debería decir que, como mínimo, se daba una ambigüedad latente a este respecto. En un mundo donde las elecciones eran sumamente costosas y la comunicación era complicada, la democracia tenía que arreglárselas con elecciones poco frecuentes. Sin embargo, no podemos saber realmente cómo habrían reaccionado los redactores de la Constitución ante una tecnología que permite la consulta perfecta y continua.

Existe una razón importante para mantenerse escéptico ante este pulso instantáneo del pueblo. Tal pulso no es cuestionable porque el pueblo sea inculto o incapaz de tener buen juicio, ni porque la democracia tenga que fallar necesariamente, sino porque a menudo es producto de la ignorancia. En efecto, a menudo la gente adopta puntos de vista desinformados o parcialmente informados que se limitan a repetir como juicios propios, cuando saben que sus auténticos juicios no van a ser tenidos especialmente en cuenta.

La tecnología alienta esto. Como consecuencia del incremento masivo de programas informativos, hoy estamos expuestos a una gama de información sobre el mundo mayor que nunca. Esta exposición, a su vez, nos proporciona confianza en nuestro juicio. Así, si la gente jamás ha oído hablar de Timor Oriental, es posible que responda a quien le pregunte: «No sé»; pero basta con que haya visto diez segundos en televisión o treinta líneas en un portal de noticias de Internet para que se forme una apreciación al respecto de la que carecía antes. Y la gente se dedica a repetir tal apreciación, sin añadirle apenas nada de cosecha propia.

La solución a este problema no consiste en reducir la cantidad de noticias o en prohibir los sondeos, sino en llevar a cabo mejores sondeos. El gobierno reacciona a la información procedente de los malos sondeos porque es la única de la que dispone, pero esos sondeos no son los únicos posibles. Existen técnicas de sondeo que compensan los errores de los sondeos instantáneos y producen juicios más ponderados y estables.

Un ejemplo de ello es el sondeo «deliberativo» concebido por el profesor James Fishkin. En lugar de tomar el pulso a la población, los sondeos de Fishkin se dedican a buscar un equilibrio,[11] reuniendo durante un fin de semana a una muestra representativa de la población. De manera previa al sondeo, a estas personas se les proporciona información para asegurarse de que saben algo sobre el asunto en cuestión; a continuación, se las divide en pequeños jurados que, a lo largo de dos días, discuten sobre dicho asunto e intercambian puntos de vista sobre la mejor manera de resolverlo. Al final de este proceso se le pregunta a la gente por sus opiniones, constituyendo sus respuestas finales los «resultados» del sondeo.

---

11 Véase, por ejemplo, James S. Fishkin, *The Voice of the People*, New Haven (Conn.), Yale University Press, 1995. Para una obra excelente que explora cómo el ciberespacio podría fomentar este proyecto general, véase Simone Beth Noveck, «Designing Deliberative Democracy in Cyberspace: The Role of the Cyber-Lawyer», *Boston University Journal of Science and Technology Law*, núm. 9, 2003, p. 1.

La gran ventaja de este sistema no radica sólo en que se obtiene información, sino en que se trata de un proceso deliberativo, donde los resultados surgen de los razonamientos de ciudadanos que debaten con otros ciudadanos. Así, no se incita a la gente exclusivamente a votar, sino a explicar las razones de su voto, razones que pueden o no llegar a convencer al resto.

Podríamos imaginar (o soñar) que este proceso se extendiese en general, que se convirtiese en un elemento básico de nuestra vida política —tal vez en una regla de ciudadanía. Si así fuera, podría resultar beneficioso como contrapeso al pulso instantáneo y al proceso perpetuamente interesado en que consiste el desempeño gubernamental ordinario. Constituiría un correctivo al proceso que ahora tenemos, un correctivo que podría aportarnos esperanza.

El ciberespacio podría aumentar las posibilidades de este proceso; y ciertamente lo hace aún más necesario. Es posible imaginar el uso de la arquitectura del espacio para diseñar foros deliberativos, los cuales podrían utilizarse para implementar los sondeos de Fishkin. Pero mi mensaje fundamental es que el ciberespacio hace de lo más urgente la necesidad de este tipo de sondeos.[12]

Existe cierta magia en un proceso donde los razonamientos cuentan —no donde los expertos imponen sus dictados o sólo la gente inteligente vota, sino donde el poder es confrontado con la razón. La magia reside en un proceso en que los ciudadanos esgrimen sus razones y son conscientes de que ese poder está restringido por tales razones.

Se trata de la magia sobre la que escribió Tocqueville cuando describió al mundo el asombroso sistema de jurados populares que existía en EEUU. Los ciudadanos que componían los jurados debían plantear argumentos razonados y convincentes para alcanzar decisiones que a menudo poseían extraordinarias consecuencias para la vida social y política. En 1835, Tocqueville escribía así acerca de estos jurados:

---

12 Dean Henry H. Perritt Jr. proporciona una idea bien desarrollada de lo que podría ser la «autorregulación» en el contexto de Internet, inspirándose en importantes ideales democráticos, véase «Cyberspace Self-government: Town Hall Democracy or Rediscovered Royalism?», *Berkeley Technology Law Journal*, núm. 12, 1997, p. 413. Según su descripción, la posibilidad de autogobierno depende en gran medida de las características arquitectónicas de la Red –y no todas se están desarrollando de modo que respalden la democracia; véase también *The Control Revolution*, *op. cit.*, pp. 150-157, 217-230, donde Shapiro discute «la política de pulsación automática» y las herramientas democráticas.

> El jurado [...] sirve para comunicar el espíritu de los magistrados a las mentes de todos los ciudadanos; y este espíritu, con los hábitos que le asisten, constituye la más sólida preparación para las instituciones libres. Infunde a todas las clases respeto hacia lo que se juzga y a la noción de derecho. [...] Enseña a los hombres a practicar la equidad; cada hombre aprende a juzgar a su prójimo como él mismo sería juzgado. [...] El jurado enseña a cada hombre a no retroceder ante la responsabilidad de sus propias acciones y le inculca la confianza varonil sin la que ninguna virtud política puede existir. Inviste a cada ciudadano con una suerte de magistratura; hace sentir a todos los deberes que han de cumplir con respecto a la sociedad, así como la parte que les corresponde en su gobierno. Al obligar a los hombres a dirigir su atención a otros asuntos distintos de los suyos, erradica ese egoísmo privado que corroe la sociedad.[13]

Sin embargo, no fue Tocqueville, ni cualquier otro teórico, quien me infundió este ideal. Fue un jurista quien me hizo ver por primera vez la fuerza de esta idea —un abogado de Madison, Wisconsin, mi tío Richard Cates.

Vivimos en una época en la que la gente sensata vilipendia a los abogados. No cabe duda de que éstos tienen parte de responsabilidad. Sin embargo, no puedo aceptar esa postura, y no sólo porque me gano la vida formando a abogados, sino porque permanece grabada en mi memoria una imagen que evocó mi tío para explicarme por qué era abogado. En 1974 acababa de regresar de Washington, donde trabajó en el Comité de Impugnación —de Nixon, no de Clinton, aunque Hillary Clinton trabajaba por entonces con él. Yo le insistí en que me contara todo, quería enterarme de las batallas políticas. No era un asunto del que se discutiera mucho en casa. Mis padres eran republicanos, pero mi tío, no.

El trabajo de mi tío consistía en presentar a los congresistas los hechos del caso —esto es, en asimilar primero todo lo que se sabía del caso para luego explicárselo a los miembros del comité. Aunque hubo muchos detalles en su relato que jamás olvidaré, la parte más fascinante no era la relacionada con la impugnación. Mi tío me estaba describiendo la esencia de su trabajo —tanto para el Comité como para sus clientes:

> Lo que hace un abogado, lo que hace un buen abogado, es lo que permite que este sistema funcione. No se trata de una simulación, ni de provocar indignación, ni de estrategias y tácticas, sino de algo mucho más sencillo. Lo que hace un buen abogado es contar una historia que convenza. No ocultando la verdad o excitando las emociones, sino usando la razón, a través de una historia, para convencer.

---

13 Tocqueville, *Democracy in America*, vol. 1, *op. cit.*, pp. 284-285.

Cuando esto funciona, provoca algo en las personas que experimentan la persuasión. Algunas de ellas, por primera vez en su vida, contemplan cómo el poder queda limitado por la razón. Ni por los votos ni por la riqueza ni por la gente que se conoce, sino por un argumento que convence. Ésta es la magia de nuestro sistema, por más raros que puedan ser los milagros.

Esta imagen se queda grabada —no en su versión elitista de expertos que deciden qué es lo mejor, ni en su versión populista de muchedumbres alborotadas abatiendo a gritos a sus oponentes, sino en la sencilla versión que conocen los miembros de los jurados populares. Y es precisamente esta sencilla imagen la que pasa por alto nuestra actual democracia; una imagen de cómo, a través de la deliberación, el entendimiento y un proceso de construcción de comunidad, se llega a los juicios acerca del modo de seguir adelante.

Podríamos reintegrar algo de esto en nuestra democracia. Cuanto más hagamos en este sentido, menos importantes serán aquellos pulsos instantáneos; y cuanto menos importantes sean éstos, tanto más podremos recobrar la fe en aquella parte de nuestra tradición que nos convirtió en revolucionarios en 1789 —el compromiso con una forma de gobierno que respeta la deliberación y al pueblo, y que se opone a la corrupción revestida de ornatos aristocráticos.

18. Lo que Declan no capta

DECLAN MCCULLAGH ES UN ESCRITOR que trabaja para *Wired News*. También dirige una lista de correo que distribuye a sus suscriptores los boletines que él decide enviar y facilita el debate entre sus miembros. La lista se denominó originalmente *Fight Censorship* (combate la censura) y atrajo en sus inicios a un gran número de suscriptores ansiosos por organizarse para resistirse a los esfuerzos estatales por «censurar» la Red.

Sin embargo, Declan ha convertido la lista en algo más que un foro de debate sobre la censura, distribuyendo en ella otras noticias que cree que gustarán a sus suscriptores. Así pues, junto a noticias sobre los esfuerzos para eliminar la pornografía de la red, Declan incluye otras referentes a los pinchazos telefónicos del FBI, a las campañas de protección de la privacidad o a los esfuerzos estatales para aplicar las leyes antimonopolio de la nación. Yo estoy suscrito a esta lista y disfruto con los mensajes que se publican.

Las ideas políticas de Declan están claras. Es un inteligente liberal cuya primera reacción ante cualquier sugerencia que implique al Estado es el desdén. En uno de sus mensajes citó la historia de un proveedor de servicios de Internet británico que violó las leyes relativas al envío masivo de faxes no solicitados; esto, alegaba Declan, demostraba la inutilidad de las leyes que regulan el correo basura. En otro mensaje criticaba los esfuerzos de Reporteros Sin Fronteras (RSF) por aprobar leyes para proteger la libertad de expresión a escala internacional.[1] Hay un tema que unifica en los

[1] Mensaje de Declan McCullagh, «Reporters Without Borders calls for regulation of US Internet companies», disponible en http://www.politechbot.com/2006/01/12/reporters-without-borders.

mensajes de Declan: dejen la Red en paz. Y con un aire socarrón, en ocasiones pretencioso, ridiculiza a aquéllos que cuestionan esta simple, aunque poderosa, idea.

He seguido la lista de Declan algún tiempo; durante un breve periodo, hace ya mucho, también seguí el foro de debate de la lista. Y a lo largo de los años que he tenido el placer de aprender de Declan, un único y sencillo mensaje ha dominado los hilos de discusión: «No hay que limitarse a preguntar», Declan insiste una y otra vez, «si existen "fallos de mercado" que exigen la intervención del Estado; también hay que preguntarse si existen "fallos del Estado"». (Como apuntó en un correo reciente sobre RSF: «Julien Pain es capaz de identificar todos estos presuntos ejemplos de fallos de mercado, pero no de identificar los fallos del Estado»). Y la consecuencia que Declan extrae de esta segunda parte de la pregunta es (como casi siempre) la recomendación de que no hagamos nada.

La pregunta de Declan tiene un excelente pedigrí. Se trata de la misma pregunta de la que partió Ronald Coase en el trabajo que le llevó al Premio Nobel. Economistas como Pigou habían identificado bienes que los mercados no podían proporcionar, lo cual bastó a Pigou para demostrar que, en consecuencia, los Estados deberían intervenir. Pero como afirmó Coase:

> Al elegir entre ordenamientos sociales en el contexto en el que se toman las decisiones individuales, debemos tener presente que un cambio del sistema existente que lleve a mejorar algunas decisiones puede también llevar a empeorar otras. Además, debemos tener en cuenta los costes que conlleva dirigir los diversos ordenamientos sociales (ya sea el funcionamiento de un mercado o de un departamento gubernamental), así como los costes que conlleva el paso a un nuevo sistema. Al concebir y elegir entre ordenamientos sociales, deberíamos considerar el efecto total.[2]

Coase se impuso una disciplina en su trabajo, que consistía en no detenerse jamás en su reflexión teórica. Los elementos teóricos son cruciales para el progreso, pero confrontar esa teoría con un poco de vida del mundo real resulta igualmente crucial.

He aquí el problema que se da con el mundo de, al menos, algunos liberales. Podemos especular hasta que las ranas críen pelo sobre cómo sería el mundo si una pandilla de liberales puros diseñara el Estado. Porque Estado

2 Ronald Coase, «The Problem of Social Cost», *Journal of Law and Economics*, octubre de 1960.

habría, por supuesto, ya que los liberales no son anarquistas. Y, sin lugar a dudas, las consecuencias de tal transformación resultarían contrarias a la intuición. Ciertamente no serían tan malas como predicen los estatistas, pero dudo que fueran tan buenas como prometen los liberales.

Sea como fuere, la realidad es que nunca vamos a vivir en un mundo liberal. Por lo tanto, la pregunta que deberíamos plantear es qué actitud deberíamos adoptar ante la regulación, *dado que vivimos en un mundo donde va a existir regulación*. ¿Debería ser nuestra respuesta en ese mundo —es decir, en este mundo y en todos los mundos posibles que vamos a llegar a ver— la de actuar como si nos opusiéramos por principio a toda regulación?

Porque si ésta es nuestra respuesta, tal actitud producirá un efecto. No paralizará toda la regulación, pero paralizará cierta forma de regulación. O mejor dicho, es seguro que *no* paralizará cierta forma de regulación —la regulación que beneficia, por ejemplo, a poderosos intereses particulares.

Consideremos un ejemplo obvio.

Los economistas estiman que nuestra economía pierde miles de millones de dólares por el lastre del correo basura. La consultora Ferris Research, por ejemplo, calcula que los costes actuales de combatir el correo basura (incluyendo la pérdida de productividad) oscilan entre 9 y 10 dólares por usuario cada mes, lo que supone casi 1.000 millones de dólares anuales.[3] Estos costes los han asumido todos los que usan una cuenta de correo electrónico de pago. Y dicho cálculo no incluye los costes indirectos derivados de perder un mensaje porque es filtrado o ignorado. (Tampoco incluye el beneficio del correo basura, pero como no voy a considerar dicho beneficio en el ejemplo comparativo, dejaré este aspecto por ahora).

Los economistas también han tratado de estimar el coste que supone a la industria, la «piratería» de contenidos bajo copyright (excluyendo el software) a través de Internet. Algunos calculan que los costes son en realidad bajos. Felix Oberholzer y Koleman Strumpf, por ejemplo, concluyeron que la compartición de archivos produce «un efecto en las ventas estadísticamente indistinguible de cero».[4] Otras estimaciones concluyen que existe una

---

3 «Study: Spam Costs Businesses $13 Billion», CNN.COM, 5 de enero de 2003, disponible en http://www.cnn.com/2003/TECH/biztech/01/03/spam.costs.ap.

4 Felix Oberholzer y Koleman Strumpf, «The Effect of File Sharing on Record Sales: An Empirical Analysis», Documento de Trabajo, núm. 3, 2004.

pérdida real, pero no enorme. En 2003, y mediante el uso de un modelo sofisticado para medir las pérdidas derivadas de la compartición de archivos durante ese mismo año, David Blackburn concluyó que la industria perdió 330 millones de dólares.[5] Esta cifra es significativamente inferior a la estimación de la RIAA (*Recording Industry Association of America*, Asociación de la Industria Discográfica de Estados Unidos) del coste total anual derivado de «todas las formas de piratería»: 420 millones de dólares.[6]

Con esto basta para comprobar que dichas estimaciones son controvertidas. Pero incluso así, hay algo absolutamente seguro en este terreno de controversia: el coste de la «piratería» es significativamente menor que el del correo basura. De hecho, el coste total de dicho correo basura —para consumidores y empresas conjuntamente— excede al total de ingresos anuales de la industria discográfica.[7]

Entonces, ¿cómo casa esta diferencia de perjuicios con lo que el Congreso ha hecho para responder a cada uno de estos problemas?

En los últimos diez años, el Congreso ha aprobado exactamente un solo proyecto de ley con el fin de abordar el problema del correo basura: la Ley CAN-SPAM de 2003. En el mismo periodo de tiempo, el Congreso ha aprobado veinticuatro leyes que afectan al copyright.[8] Por supuesto no todas estas leyes apuntan directamente a la «piratería», pero todas ellas se dirigen a proteger de forma más amplia las obras bajo copyright en la era digital.

---

5 David Blackburn, «On-line Piracy and Recorded Music Sales», Harvard University, Job Market Paper, 2004, disponible en www.katallaxi.se/grejer/blackburn/blackburn_fs.pdf.

6 Recording Industry Association of America Home Page, «Issues-Anti-Piracy: Old as the Barbary Coast, New as the Internet», disponible en http://www.riaa.com/issues/piracy/default.asp.

7 David Blackburn, «On-line Piracy and Recorded Music Sales», *op. cit.*

8 *Family Entertainment and Copyright Act* de 2005 (P.L. 109–9), promulgada el 27 de abril de 2005 (añade la sección 2319B al Título 17, estipulando como delito punible con prisión la copia sin autorización en salas de cine de películas o cualquier otra obra audiovisual amparada en el Título 17); *Intellectual Property Protection and Courts Amendment Act* de 2004 (P.L. 108–482), promulgada el 23 de diciembre de 2004 (enmienda a la Ley de Marcas Registradas de 1946 para estipular penas criminales y civiles elevadas a aquellos individuos que presenten, intencionadamente a una autoridad de registro de nombres de dominio, información falsa relativa a una dirección de Internet empleada para cometer un crimen o incurrir en infracciones, a través de Internet de la legislación de copyright o de marcas registradas); *Satellite Home Viewer Extension and Reauthorization Act* de 2004 (contenida en la *Consolidated Appropriations Act*, 2005, P.L. 108–447), promulgada el 8 de diciembre de 2004 (además de extender por un periodo adicional de cinco años la licencia estatutaria de las operadoras de satélite que retransmiten contenidos de cadenas de televisión a sus suscriptores, y de introducir algunas enmiendas a la vigente

Esta pauta no es accidental. En un mundo político dominado como lo está el nuestro, el proceso legislativo se pone en marcha cuando beneficia a intereses específicos, y no se pone en marcha cuando se opone a ellos. Y en estos dos ejemplos, tanto la falta de regulación como la plétora de regulación se explican precisamente por esta cuestión. Ha habido veinticuatro proyectos de ley sobre el copyright porque las «estrellas de rock» han presionado en ese sentido; y ha habido un solo proyecto de ley relativo al correo basura porque los remitentes de publicidad directa (y muchas grandes compañías) prestaron declaración en su contra.

Pues bien, dada esta realidad, sugiero que los liberales deberían reconocer un tercer fallo importante que complementa los fallos «de mercado» y «de Estado»: el «fallo de mercado» se da cuando no puede esperarse que los mercados proporcionen determinados bienes de forma eficaz; el «fallo de Estado» se da cuando no puede esperarse que el Estado solucione los fallos de mercado de forma eficaz; y el «fallo liberal» se da cuando la presión para no hacer nada no produce una ausencia absoluta de regulación, sino una regulación por parte de los intereses específicos más poderosos. O expresado en forma de eslogan: si consideramos erróneo presionar a favor de la regulación, sólo los intereses erróneos conseguirán regulación.

---

sección 119 de la Ley de Copyright, esta ley ordena a la Oficina de Copyright llevar a cabo dos estudios y comunicar sus hallazgos a la Comisión de Justicia de la Cámara de Representantes y a la Comisión de Justicia del Senado; uno de ellos, encargado para finales del año 2005, exigía que la Oficina examinara porciones específicas de la licencia recogida en la sección 119, y que determinara qué impacto, si es que había alguno, habían producido las secciones 119 y 122 en los titulares del copyright cuyos programas televisivos retransmitían las operadoras de satélite); *Individuals with Disabilities Education Improvement Act* de 2004 (P.L. 108–446), promulgada el 3 de diciembre de 2004 (modifica la sección 121 del Título 17, estipulando el establecimiento del NIMAS –*National Instructional Materials Accessibility Center*, Centro Nacional de Accesibilidad a Materiales Instructivos– y la accesibilidad libre a determinados materiales —tales como materiales en Braille, grabaciones sonoras o textos digitales para uso de personas con ceguera— a través del NIMAS); *Copyright Royalty and Distribution Reform Act* de 2004 (P.L. 108–419), promulgada el 30 de noviembre de 2004 (enmienda la Ley de Copyright para reemplazar el sistema del tribunal de arbitraje de regalías de la Oficina de Copyright, creado en cumplimiento de la *Copyright Royalty Tribunal Reform Act* de 1993, por tres juzgados de regalías que supervisen el ajuste de las tarifas de las regalías de las licencias obligatorias y la distribución de dichas regalías); *Small Webcaster Settlement Act* de 2002 (P.L. 107–321), promulgada el 4 de diciembre de 2002 (enmienda la Ley de Copyright para establecer derechos de regalías por actuaciones para las grabaciones sonoras transmitidas mediante tecnología electrónica digital); *Technology, Education, and Copyright Harmonization Act* de 2002 (P.L. 107–273, Subtítulo C de la *21st Century Department of Justice Appropriations Authorization Act*), aprobada el 2 de noviembre de 2002 (introduce disposiciones relativas al uso de obras bajo copyright con fines de educación a distancia); *Intellectual Property and High Technology Technical Amendments Act* de 2002 (P.L. 107–273, Subtítulo B de la *21st Century Department of Justice Appropriations Authorization*

Yo no soy un liberal en el sentido en el que lo es Declan, aunque comparto su escepticismo acerca del Estado. Ahora bien, no podemos traducir tal escepticismo en dejadez. Tenemos por delante un montón de decisiones que influirán en el modo en que se desarrollará Internet y en los principios que ésta encarne. La actitud que obvia al Estado en la toma de dichas decisiones no impedirá que éste intervenga, sino que simplemente impedirá que lo haga para tomar las decisiones correctas.

Desde mi punto de vista, los Estados deberían intervenir, como mínimo: cuando la acción privada acarree repercusiones públicas negativas; cuando las acciones de miras estrechas amenacen con causar daños a largo plazo;

Act), aprobada el 2 de noviembre de 2002 (realiza correcciones técnicas al Título 17 y a la *IP and Communications Omnibus Reform Act* de 1999, también conocida como la *Satellite Home Viewer Improvement Act* de 1999); *Work Made for Hire and Copyright Corrections Act* de 2000 (P.L. 106–379), aprobada el 27 de octubre de 2000 (enmienda la definición de obras del Título 17); *Digital Theft Deterrence and Copyright Damages Improvement Act* de 1999 (P.L. 106–160), aprobada el 9 de diciembre de 1999 (incrementa los daños estatutarios por infracción del copyright mediante la enmienda del capítulo 5 del Título 17); *Satellite Home Viewer Improvement Act* de 1999 (P.L. 106–113), aprobada el 29 de noviembre de 1999 (enmienda los capítulos 12 y 13 del Título 17); *Copyright Amendments and Amendments to the Vessel Hull Design Protection Act* (P.L. 106–44), aprobada el 5 de agosto de 1999 (realiza correcciones técnicas al Título 17); *Vessel Hull Design Protection Act* (P.L. 105–304, Título V de la *Digital Millennium Copyright Act*), aprobada el 28 de octubre de 1998 (introduce protección de diseño para los cascos de navíos); *Computer Maintenance Competition Assurance Act* (P.L. 105–304, Título III de la *Digital Millennium Copyright Act*), aprobada el 28 de octubre de 1998 (enmienda la sección 117 del Título 17); *Online Copyright Infringement Liability Limitation Act* (P.L. 105–304, Título III de la *Digital Millennium Copyright Act*), aprobada el 28 de octubre de 1998 (añade la sección 512 al Título 17); *WIPO Copyright and Performances and Phonograms Treaties Implementation Act* of 1998 (P.L. 105–304, Título I de la *Digital Millennium Copyright Act*), aprobada el 28 de octubre de 1998 (añade un nuevo capítulo 12 al Título 17, el cual prohíbe sortear los sistemas de protección del copyright y estipula la protección para la información de gestión del copyright); *Digital Millennium Copyright Act* (P.L. 105–304), aprobada el 28 de octubre de 1998; *Fairness in Music Licensing Act* de 1998 (P.L. 105–298), aprobada el 27 de octubre de 1998 (enmendando la sección 110 y añadiendo la sección 513 para proporcionar una exención de la licencia de música a los establecimientos de servicio de comida y de bebida); *Sonny Bono Copyright Term Extension Act* (P.L. 105–298, Título I), aprobada el 27 de octubre de 1998 (extiende el periodo de protección del copyright para la mayoría de las obras a 70 años después de la muerte del autor); *No Electronic Theft (NET) Act* (P.L. 105–147), aprobada el 16 de diciembre de 1997; *Copyright Amendments and Amendments to Semiconductor Chip Protection Act* de 1984 (P.L. 105–80), aprobada el 13 de noviembre de 1997 (introduce enmiendas técnicas a ciertas disposiciones del Título 17); *Legislative Branch Appropriations Act* (P.L. 104–197), aprobada el 16 de septiembre de 1996 (añade una nueva versión de la sección 121 referente a la limitación en el copyright para obras literarias en formatos especializados para personas con ceguera o discapacidad); *Anticounterfeiting Consumer Protection Act* de 1996 (P.L. 104–153), aprobada el 2 de julio de 1996 (enmienda la sección 603 del Título 17 y la sección 2318 del Título 18); *Digital Performance Right in Sound Recordings Act* de 1995 (104–139), aprobada el 1 de noviembre de 1995 (enmienda la sección 114 y 115 del Título 17).

cuando la falta de intervención socave importantes principios constitucionales y derechos individuales; cuando surja una forma de vida que pueda amenazar aquellos principios que consideramos fundamentales; y cuando podamos ver que dicha falta de intervención a favor de lo justo se limitará a fortalecer las intervenciones a favor de lo injusto. En tales casos, la intervención estatal debe ser limitada y no perder de vista toda la conciencia sobre los fallos del Estado que la gente juiciosa pueda acumular. Ahora bien, la acción que defiende lo justo no debería detenerse simplemente porque algo salga mal. Cuando aquéllos que creen en la libertad del ciberespacio y en los principios que tal libertad promueve, se niegan a implicarse con el Estado en la búsqueda de la mejor manera de preservar dichas libertades, ello debilita la libertad. La inacción no constituye una respuesta; puede y debe hacerse algo.

Yo defiendo esto, pero sin demasiada esperanza. Los Declans tienen un papel tan central en nuestra cultura política actual que me confieso incapaz de hallar un modo de eludirlo. He bosquejado algunos pequeños pasos, pero parecen insignificantes; he descrito un ideal diferente, pero parece bastante extraño; he prometido que podría hacerse algo diferente, pero ninguna de las instituciones de gobierno que conozco es capaz de ello.

La verdad, sospecho, es que los Declans vencerán —al menos por ahora. Trataremos los desastres medioambientales basados en el código —como la pérdida de privacidad, la censura por parte de los filtros censores o la desaparición del procomún intelectual— como si fueran producidos por dioses y no por el ser humano. Contemplaremos cómo la emergente arquitectura de tipo panóptico elimina aspectos importantes de la privacidad y de la libertad de expresión, y afirmaremos, como modernos Jeffersons, que la naturaleza lo ha hecho así —olvidando que aquí nosotros somos la naturaleza. En muchos ámbitos de nuestra vida social, llegaremos a ver la Red como el producto de algo extraño —algo que no podemos controlar porque no podemos controlar nada, algo que más bien debemos limitarnos a aceptar a medida que invade y transforma nuestras vidas.

Hay quien asegura que vivimos una época emocionante, pero se trata de la emoción del adolescente que, desafiando a otro conductor que viene en dirección contraria, se lanza a todo gas por la autopista y suelta las manos del volante. Hay decisiones que podríamos tomar, pero fingimos que no podemos hacer nada al respecto. Elegimos fingir, cerramos los ojos. Nos dedicamos a construir esta naturaleza, y luego quedamos constreñidos por la naturaleza que nosotros hemos construido.

Vivimos en la época del avestruz. Nos sentimos emocionados por lo que no podemos conocer. Estamos orgullosos de dejar las cosas a merced de la mano invisible. Y somos nosotros quienes la volvemos invisible al mirar hacia otro lado.

No se trata de una época propicia, culturalmente hablando, para enfrentarse a tecnologías revolucionarias. No estamos más preparados para esta revolución de lo que los soviéticos lo estaban para la suya. A nosotros, como a ellos, una revolución nos ha cogido por sorpresa. Pero nosotros, a diferencia de ellos, sí tenemos algo que perder.

Apéndice

En el Capítulo 7 esbocé brevemente un argumento sobre cómo las cuatro modalidades de regulación descritas restringen de forma diferente; en este apéndice quiero ampliar aquel razonamiento. Albergo la esperanza de proporcionar más sentido al modo en que estas modalidades —la ley, el mercado, las normas y la arquitectura— interactúan en la regulación. Tal comprensión resulta útil, aunque no necesaria, para captar el argumento de este libro. Es por ello que la he incluido aquí, para aquéllos que tengan interés y tiempo de sobra. En otro lugar he denominado a este enfoque «la Nueva Escuela de Chicago».[1]

La ley es una orden respaldada por la amenaza de una sanción. Nos ordena no cometer un asesinato y nos amenaza con una severa pena si lo hacemos pese a todo. O nos ordena no traficar con cocaína y nos amenaza con castigos bárbaros si lo hacemos. En ambos casos la imagen de la ley es bastante sencilla y rotunda: prohibido hacer esto, o lo otro.

Obviamente la ley es mucho más que un conjunto de órdenes y amenazas.[2] La ley no sólo ordena ciertas conductas, sino que expresa los principios de una comunidad (cuando, por ejemplo, reserva un día para celebrar el nacimiento de Martin Luther King, Jr.);[3] constituye o regula estructuras de

---

1 Lessig, «The New Chicago School», *Journal of Legal Studies*, núm. 661, 1998.

2 Véase H. L. A. Hart, *The Concept of Law* (2ª), Nueva York, Oxford University Press, 1994, pp. 6–13, 27–33 [ed. cast: *El concepto de Derecho*, trad. por Genaro R. Carrio Buenos Aires, Abeledo-Perrot, 1990].

3 Por ejemplo, la ley de Illinois establece: «El tercer lunes del mes de enero de cada año es un día de fiesta que ha de ser observado en todo el Estado y conocido como el nacimiento del Dr. Martin Luther King, Jr. Cada año en los diez días anteriores al nacimiento del Dr. Martin Luther King, Jr., el gobernador emitirá una proclamación que anuncie la festividad y designe los actos oficiales que se celebrarán para honrar la memoria del Dr. Martin Luther King, Jr., así como sus contribuciones a esta nación»; *Illinois Comprehensive Statutes Annotated* núm. 5, 490/65, West, 1998.

gobierno (cuando la Constitución, por ejemplo, establece en el Artículo I una Cámara de Representantes distinta del Senado); y establece derechos que los individuos pueden invocar frente a su propio Estado (la Declaración de Derechos). Todos estos son ejemplos de leyes, y no pretendo disminuir su relevancia al centrarme exclusivamente en un tipo de ley. Con todo, este aspecto particular de la ley establece una restricción bien definida sobre los individuos dentro de la jurisdicción del legislador o soberano. Tal restricción —objetivamente— es la amenaza de castigo.

Las normas restringen de forma diferente. Por normas sociales entiendo aquellas restricciones normativas impuestas, no a través de acciones organizadas o centralizadas por el Estado, sino a través de las múltiples sanciones sutiles y a veces enérgicas que los miembros de una comunidad se imponen entre sí. No me refiero a las pautas de conducta: puede que la mayoría de la gente vaya en coche al trabajo entre las siete y las ocho de la mañana, pero ello no constituye una norma en el sentido al que aquí aludo. Una norma gobierna la conducta socialmente relevante, convirtiendo la desviación respecto a ella en socialmente anormal.[4]

La vida está llena de, constituida por y definida en relación a tales normas —algunas de ellas valiosas, otras muchas no. Es una norma (una buena norma) agradecer a los demás sus favores. No hacerlo convierte a la persona en «grosera», y ser grosera la expone a un abanico de sanciones que van desde el ostracismo hasta la crítica. Es una norma dirigirse cautamente al compañero de asiento en un avión, o permanecer en el carril derecho cuando se conduce despacio. Las normas disuaden a los hombres de acudir al trabajo vestidos de mujer, y nos incitan a bañarnos regularmente. La vida cotidiana está repleta de este tipo de órdenes sobre cómo hemos de comportarnos. Para una persona socializada normalmente, estas órdenes constituyen una porción significativa de las restricciones sobre su conducta individual.

Así pues, las normas, al igual que la ley, constituyen reglas efectivas. Lo que hace diferentes a las normas es el mecanismo y el origen de su sanción: ellas son impuestas por una comunidad, no por un Estado. En cambio, las normas son similares a la ley en que, al menos objetivamente, su restricción se impone después de que se produzca su incumplimiento.

---

4 Véase Robert Cooter, «Expressive Law and Economics», *Journal of Legal Studies*, núm. 27, 1998, p. 585.

Las restricciones del mercado también son diferentes, pues el mercado impone sus restricciones mediante el precio. Un precio señala el punto en el que un recurso puede transferirse de una persona a otra. Si el lector quiere un café de Starbucks, debe entregar al dependiente cuatro dólares. La restricción (los cuatro dólares) es simultánea al beneficio deseado (el café). Por supuesto, el lector puede regatear para pagar más tarde el beneficio («Con mucho gusto le pagaría el próximo martes la hamburguesa de hoy»), pero se incurre en la obligación en el mismo momento en que se recibe el beneficio. En la medida en que el lector permanezca dentro del mercado, esta simultaneidad queda preservada. A diferencia de las impuestas por la ley y las normas, la restricción del mercado no entra en vigor después de que se obtenga el beneficio buscado, sino que lo hace al mismo tiempo.

Esto no equivale a decir que las transacciones mercantiles no puedan traducirse a transacciones legales o normativas. De hecho, las transacciones mercantiles sólo pueden existir dentro de un contexto legal y normativo. El lector debe pagar su café; si no lo hace, se le aplicará la ley de robo. Nada en el mercado obliga al lector a dar propina al camarero, pero si no lo hace, se le aplicarán las normas que regulan su tacañería. Las restricciones del mercado existen a causa de un elaborado trasfondo de leyes y normas que definen los bienes que se pueden comprar y vender, así como de reglas de propiedad y contratación que definen cómo se los puede comprar y vender. Pero dadas estas leyes y normas, el mercado aún restringe de un modo distinto.

La restricción de la última modalidad de regulación no es ni tan contingente ni, en su amplia gama, tan dependiente. Se trata de la restricción de la arquitectura —el modo en que se nos presenta el mundo, o aspectos específicos de él. Los arquitectos lo denominan el entorno construido; aquéllos que no asignan nombres a las cosas simplemente lo reconocen como el mundo que les rodea.

Evidentemente algunas de las restricciones de la arquitectura las hemos construido nosotros (de ahí el sentido del término «arquitectura») y otras no. Una puerta mantiene cerrada una habitación. Cuando está cerrada con llave, la puerta nos mantiene fuera de la habitación. Esta restricción no funciona como la de la ley o las normas —no es posible ignorar la restricción y sufrir luego las consecuencias. Aunque la restricción impuesta por la puerta es superable —echándola abajo, o forzando su cerradura—, la puerta sigue imponiendo su restricción, por más que no sea de forma absoluta.

Sin embargo, algunas restricciones arquitectónicas sí son de carácter absoluto. A pesar de lo que se ve en *Star Trek*, no se puede viajar a «velocidad de curvatura». Podemos viajar rápido y la tecnología nos ha permitido

hacerlo. No obstante, tenemos razones de peso (o al menos los físicos las tienen) para creer que hay un límite de velocidad, la velocidad de la luz, que no podemos rebasar. Tal como lo expresaba una camiseta que vi en el MIT: «186.282 millas por segundo. No sólo es una buena idea. Es la ley».

Pero independientemente de que estas restricciones sean o no absolutas, o de que sean naturales o artificiales, podemos englobarlas en una misma clase —las restricciones de la arquitectura, o el código del espacio real. Lo que unifica dicha clase es el agente de la restricción: ningún individuo ni ningún grupo impone la restricción, o al menos no de forma directa. Sin duda los individuos son los responsables últimos de buena parte de las restricciones, pero las propias restricciones se valen por sí mismas para su ejecución real. Las leyes necesitan de policías, fiscales y tribunales para surtir efecto; una cerradura no. Las normas requieren que los individuos tomen nota de las conductas discordantes y respondan como corresponde; la gravedad no. Las restricciones de la arquitectura son autoejecutables de un modo que no lo son las de la ley, las normas y el mercado.

Este rasgo de la arquitectura —la autoejecución— es extremadamente importante para entender su papel en la regulación. Además, resulta particularmente importante para la regulación deshonesta o injusta. Por ejemplo, en la medida en que podemos dar lugar a efectos a través de las restricciones automáticas del código del espacio real, no necesitamos depender de la actividad, lealtad o responsabilidad permanente de los individuos. Si logramos que una máquina se ocupe de eso, podemos estar seguros de que se introducirán regulaciones deshonestas.

El lanzamiento de misiles nucleares constituye un buen ejemplo de ello. En su concepción original, los misiles debían ser lanzados por miembros del ejército situados dentro de los silos de lanzamiento de misiles. Estos hombres recibirían la orden de lanzamiento y la expectativa era que la cumplieran. Las leyes, por supuesto, respaldaban dicha orden de lanzamiento —desobedecerla implicaba ser sometido a un consejo de guerra.[5]

Sin embargo, al probar el sistema, el ejército lo encontró cada vez menos fiable. La decisión de lanzar un misil nuclear siempre quedaba sometida al juicio de un individuo, que tenía que decidir si debía obedecer la orden.

---

[5] Cf. Paul N. Bracken, *The Command and Control of Nuclear Forces*, New Haven, Yale University Press, 1983, pp. 179–237; Christopher Chant y Ian Hogg, *The Nuclear War File*, Londres, Ebury Press, 1983, pp. 68–115.

Evidentemente este sistema resulta menos fiable que uno en el que todos los misiles estén conectados, como así lo estaban, con un único botón situado en el escritorio del Presidente. Pero podríamos creer que existe un valor en esta segunda comprobación, que la delegación del lanzamiento en un soldado asegura cierta revisión adicional sobre la decisión de lanzar un misil nuclear.[6]

Ésta es una consecuencia importante de la naturaleza automática de las restricciones arquitectónicas. La ley, las normas y el mercado representan restricciones revisadas mediante el juicio, que sólo se aplican cuando ciertos grupos o personas deciden hacerlo. En cambio, las restricciones que impone la arquitectura, una vez instituidas, producen su efecto hasta que alguien las detiene.

El agente de la restricción constituye, pues, un factor de distinción entre estas cuatro modalidades. La temporalidad de la restricción (cuándo es impuesta) es un segundo factor.

Aquí debería distinguir entre dos perspectivas: la de quien observa cómo se impone la restricción (la perspectiva objetiva) y la de quien experimenta la restricción (la perspectiva subjetiva). Hasta el momento mi descripción de las cuatro modalidades de restricción en este modelo único se ha limitado a la perspectiva objetiva. Desde esta perspectiva las cuatro modalidades son bastante diferentes, pero desde una perspectiva subjetiva no tienen por qué diferir en absoluto.

Desde la perspectiva objetiva, la diferencia se da entre restricciones que demandan el pago en el momento y restricciones que permiten actuar primero y pagar después. La arquitectura y el mercado pertenecen al primer tipo, mientras que la ley y las normas pertenecen al segundo. Pensemos, por ejemplo, en las restricciones que nos bloquean el acceso a la casa con aire acondicionado de nuestro vecino cuando éste se marcha el fin de semana. La ley nos restringe —si irrumpimos en su casa, constituirá allanamiento de morada. Las normas también —no es de buena vecindad irrumpir en casa de un vecino sin su permiso. Ahora bien, estas dos restricciones nos serían impuestas después de irrumpir en su casa, siendo precios que tendríamos

---

6 Por otro lado, el ejército incorporó al sistema mecanismos tecnológicos de bloqueo de la capacidad de lanzamiento, con el fin de asegurar que ninguna decisión de lanzamiento fuese nunca demasiado fácil; véase también Daniel Ford, *The Button: The Nuclear Trigger—Does It Work?*, Londres, Allen and Unwin, 1985, pp. 118–121.

que pagar a posteriori.[7] La restricción de la arquitectura equivale a la cerradura de la puerta —nos bloquea en el momento en que intentamos penetrar en la casa. El mercado restringe nuestra posesión de un aparato de aire acondicionado de la misma manera —nos demanda dinero antes de entregárnoslo. Desde una perspectiva objetiva, lo que distingue a estas dos clases de restricciones es su temporalidad —esto es, cuándo se impone la sanción.

Desde una perspectiva subjetiva, en cambio, todas estas diferencias pueden desaparecer. Subjetivamente es muy posible que sintamos la restricción de una norma mucho antes de violarla. Podemos sentir la restricción contra la irrupción en casa del vecino desde el mismo momento en que lo pensamos. Así pues, una restricción puede darse objetivamente a posteriori, pero experimentarse subjetivamente a priori.

Esta idea no se limita a las normas. Pensemos en los niños y el fuego. El fuego es un fragmento del código del espacio real: sus consecuencias se sienten tan pronto como se violan las restricciones que él impone. Un niño aprende esto la primera vez que acerca la mano a la llama. A partir de aquí, el niño interioriza la restricción del fuego antes de acercar la mano a él: habiéndose quemado ya una vez, el niño sabe que no debe acercar la mano a la llama una segunda vez.[8]

---

7 «Los fenómenos de significado social y de inconmensurabilidad restringen la elección racional (tanto individual como colectiva). Generalizando, resulta irracional tratar los bienes como conmensurables cuando el uso de una métrica cuantitativa elimina ciertas dimensiones de significado que son esenciales para los propósitos u objetivos de una persona. Sería irracional, por ejemplo, que una persona que quisiera convertirse en un buen colega en el seno de una comunidad académica ofreciera a otra investigadora dinero, en lugar de comentarios, a cambio de su manuscrito. Con el trasfondo de las normas sociales, el sentido de respeto que implican los comentarios no puede reproducirse mediante cantidad alguna de dinero; el mero hecho de intentar tal sustitución comunica que esa persona no valora a su colega de un modo acorde con su relación»; Dan M. Kahan, «Punishment Incommensurability», *Buffalo Criminal Law Review*, núm. 1, 1998, pp. 691, 695.

8 Muchos eruditos, entre ellos principalmente Robert Cooter, sostienen que las normas son especiales porque son «interiorizadas» en un sentido en que no lo son las otras restricciones; véase Robert D. Cooter, «Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant», *University of Pennsylvania Law Review*, núm. 144, 1996, pp. 1643, 1662; Robert D. Cooter, «The Theory of Market Modernization of Law», *International Review of Law and Economics*, núm. 16, 1996, pp. 141, 153. Por interiorización Cooter simplemente describe la misma clase de subjetividad que se da en el caso del niño y el fuego: se pasa de una restricción objetiva a posteriori a una restricción subjetiva a priori. La norma se convierte en parte de la persona, hasta tal punto que ésta siente su resistencia antes de actuar, de modo que dicha resistencia controla las acciones de la persona antes de que actúe. Una vez interiorizadas, las normas ya no necesitan ser ejecutadas para ejercer su fuerza; tal fuerza se ha traspasado al interior de la persona, por así decirlo, y perdura en el seno de esta perspectiva subjetiva. En mi opinión, deberíamos considerar que cada una de las restricciones

Podemos describir este cambio como el desarrollo de una restricción subjetiva sobre la conducta del niño, y así ver cómo la idea se extiende a otras restricciones. Pensemos en el mercado bursátil. Para aquéllos que no invierten en bolsa muy a menudo, es muy posible que las restricciones del mercado se reduzcan a la restricción objetiva del precio demandado al realizar una compra. En cambio, para aquéllos que experimentan en el mercado de forma regular —que poseen, por así decirlo, un sentido mercantil—, las restricciones del mercado resultan bastante diferentes. Llegan a conocerlas como si se tratara de una segunda naturaleza, la cual guía o restringe sus acciones. Pensemos en una corredora de bolsa en el parqué del mercado de valores. Ser una gran corredora de bolsa implica llegar a conocer el mercado «como la palma de su mano», dejar que se convierta en su segunda naturaleza. En los términos que hemos empleado, esta corredora ha dejado que el mercado se convierta subjetivamente en parte de su ser.

Así pues, cada una de las restricciones posee un aspecto subjetivo y otro objetivo. Las leyes funcionan objetivamente a posteriori, pero para la mayoría de nosotros el hecho de que una ley nos imponga órdenes en un determinado sentido basta para convertirla en una restricción subjetiva. (Lo que me compele a no defraudar a Hacienda no es la amenaza objetiva de la cárcel, sino más bien el hecho de que yo he convertido en subjetivas las restricciones legales con respecto a los impuestos. Lo digo en serio, responsables de Hacienda. Esto es cierto). Y en cuanto restricción subjetiva, nos restringe antes de que actuemos.

Para aquellas personas completamente maduras, o plenamente integradas, todas las restricciones objetivas son subjetivamente efectivas previamente a sus acciones. Sienten las restricciones del código del espacio real, de la ley, de las normas y del mercado antes de actuar. Para aquellas personas completamente inmaduras, o totalmente alienadas, pocas restricciones objetivas resultan subjetivamente efectivas. Estas personas se lanzan al fango y sólo entonces se enteran de las restricciones que éste impone; roban pan y sólo entonces se enteran de los castigos que impone la ley; se presentan en una boda en pantalones cortos y sólo entonces se percatan del desprecio de sus amigos; gastan todo su dinero en chucherías y sólo entonces comprenden las penurias que impone el mercado. Estos dos tipos de personas marcan los dos extremos; la mayoría de nosotros se encuentra en algún punto intermedio entre ambos.

---

funciona de la misma manera: subjetivamente llegamos a asumir la restricción a través de un proceso de interiorización. Ciertamente algunos incentivos para la interiorización pueden ser más poderosos que otros, pero ésa es la única diferencia.

Por consiguiente, cuanto más subjetiva es una restricción, tanto más efectiva resulta a la hora de regular la conducta. Convertir una restricción en subjetiva es una tarea ardua, ya que la persona debe decidir que esa restricción pase a formar parte de lo que es. En la medida en que la norma se convierte en subjetiva, impone su restricción de forma simultánea a la conducta que regula.

Esto señala una última distinción entre la ley y las normas, por un lado, y el código del espacio real, por el otro. La ley y las normas son tanto más eficaces cuanto más subjetivas son, pero necesitan un mínimo de subjetividad para llegar a ser efectivas. La persona sobre la que se impone la restricción debe conocerla. Una ley que castigase secretamente a las personas por delitos cuya existencia desconocen no sería efectiva a la hora de regular la conducta que castiga.[9]

Pero esto no sucede con la arquitectura. La arquitectura puede restringir sin necesidad de ningún mínimo de subjetividad. Una cerradura restringe al ladrón independientemente de que este sepa que hay una cerradura que bloquea la puerta. La distancia entre dos lugares restringe las relaciones entre ellos independientemente de que sus habitantes sean conscientes de tal restricción. Este argumento constituye un corolario del argumento previo acerca del agente de la restricción: del mismo modo que no es necesario que ningún agente imponga la restricción, tampoco lo es que el sujeto la comprenda.

Las restricciones arquitectónicas funcionan, pues, independientemente de que el sujeto sea consciente de ello, mientras que la ley y las normas sólo funcionan si el sujeto sabe algo de ellas. Si el sujeto las ha interiorizado, la ley y las normas pueden restringir independientemente de si el coste de acatarlas excede el beneficio de desviarse de ellas. De este modo, la ley y las normas pueden asemejarse más al código cuanto más interiorizadas estén, pero dicha interiorización requiere esfuerzo.

Aunque he usado un lenguaje que evoca el de los arquitectos, mi lenguaje no es ése. Se trata, más bien, de un lenguaje que he hurtado y distorsionado. Yo no soy un experto en arquitectura, pero he tomado de ella su visión acerca de la relación entre el entorno construido y las prácticas que ese entorno genera.[10] Ni los arquitectos ni yo mismo tomamos esta relación

---

9 Cf. Dan M. Kahan, «Ignorance of Law Is an Excuse—But Only for the Virtuous», *Michigan Law Review*, núm. 96, 1997, p. 127.

10 Véase, por ejemplo, Schuster *et al.* (ed), *Preserving the Built Heritage, op. cit.*; Peter Katz, *The New Urbanism: Toward an Architecture of Community*, Nueva York, McGraw-Hill, 1994; Duany y Plater-Zyberk (ed.), *Towns and Town-Making Principles, op. cit.*

como algo determinante. La estructura X no determina la conducta Y, sino que más bien estas formas constituyen influencias que pueden cambiar y que, cuando lo hacen, alteran la conducta afectada.

Al igual que Michael Sorkin, creo que «los sentidos están insertos en las formas, y los entornos de la vida social pueden contribuir a su desarrollo». Su libro *Local Code: The Constitution of a City at 42N Latitude* [Código local. La constitución de una ciudad a 42º norte de latitud] sugiere cada uno de los rasgos del modelo que aquí describo, incluyendo la ambigüedad entre la ley y la arquitectura (la construcción de códigos) y la constitución que ambas posibilitan. Cualquiera que sea el origen del contenido de dichos códigos, escribe Sorkin, «sus consecuencias son construidas».[11] He aquí el rasgo en que hemos de centrarnos.

Mi sugerencia es que si relativizamos los reguladores —si entendemos cómo regula cada una de las diferentes modalidades, y de qué manera todas ellas están sujetas, en un sentido importante, a la ley— entonces veremos cómo la libertad no se construye simplemente mediante los limites que establecemos en la ley, sino también por medio de las estructuras que preservan un espacio para la decisión individual, por más restringida que ésta pueda estar.

Estamos entrando en una época en la que nuestro poder para manejar las estructuras de regulación está alcanzando el punto más alto de todos los tiempos. Resulta imperativo, pues, que comprendamos qué hacer exactamente con tal poder. Y, lo que es más importante, qué no hacer con él.

---

11 Michael Sorkin, *Local Code: The Constitution of a City at 42N Latitude*, Nueva York, Princeton Architectural Press, 1993, p. 127.

Bibliografía

ABELSON, Hal *et al.*: «The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption», *WorldWideWeb Journal*, núm. 2, 1997, p. 241.

ABRAMS, Floyd: «First Amendment Postcards from the Edge of Cyberspace», *St. John's Journal of Legal Commentary*, núm. 11, 1996, p. 693.

ACKERMAN, Bruce: *Social Justice in the Liberal State*, New Haven, Yale University Press, 1980 [ed. cast.: *La justicia social en el estado liberal*, rev. por Luis Rodríguez Abascal y trad. por Carlos Rosenkrantz *et al.*, Madrid, Centro de Estudios Constitucionales, 1993].

ALDER, Robert S. y PITTLE, R. David: «Cajolery or Command: Are Education Campaigns an Adequate Substitute for Regulation?», *Yale Journal on Regulation*, núm. 1, 1984, p. 159.

AMAR, Akhil Reed: «Fourth Amendment First Principles», *Harvard Law Review*, núm. 107, 1994, p. 757.

______«The Bill of Rights as a Constitution», *Yale Law Journal*, núm. 100, 1991, p. 1131.

AMMORI, Marvin: «Another Worthy Tradition: How the Free Speech Curriculum Ignores Electronic Media and Distorts Free Speech Doctrine», *Missouri Law Review*, núm. 70, 2005, p. 59.

ANDERSON, C. y BUSHMAN, B.: «Effects of Violent Video Games on Aggressive Behavior, Aggressive Cognition, Aggressive Affect, Physiological Arousal, and Prosocial Behavior: A Meta-Analytic Review of the Scientific Literature», *Psychological Science*, vol. 12, núm. 5, 2001, pp. 353.

AOKI, Keith: «(Intellectual) Property and Sovereignty: Notes Toward a Cultural Geography of Authorship», *Stanford Law Review*, núm. 48, 1996, p. 1293.

______«Foreword to Innovation and the Information Environment: Interrogating the Entrepreneur», en *Oregon Law Review*, núm. 75, 1996.

______«Authors, Inventors, and Trademark Owners: Private Intellectual Property and the Public Domain», en *Columbia-VLA Journal of Law and the Arts*, núm. 18, 1993.

AREEDA, Phillip E. *et al.*: *Antitrust Law,* vol. 2A, Boston, Little Brown, 1995.

ARMOND, Michelle: «Regulating Conduct on the Internet: State Internet Regulation and the Dormant Commerce Clause», *Berkeley Technology Law Journal*, núm. 17, 2002, pp. 379.

ARONSON, Larry: *HTML Manual of Style*, Emeryville (Cal.), Ziff-Davis Press, 1994.

ARRISON, Sonia: «Canning Spam: An Economic Solution to Unwanted Email», Pacific Research Institute, febrero de 2004, núm. 9.

BAILEY, Jane: «Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation», *Manitoba Law Journal*, núm. 30, 2004, p. 197.

BAIRD, Douglas G., GERTNER, Robert H. y PICKER, Randal C.: *Game Theory and the Law*, Cambridge (Mass.), Harvard University Press, 1994.

BAKER, Stewart A. y HURST, Paul R.: *The Limits of Trust: Cryptography, Governments, and Electronic Commerce*, Boston, Kluwer Law International, 1998.

BARLOW, John Perry: «A Declaration of the Independence of Cyberspace», 1996, disponible en http://homes.eff.org/~barlow/Declaration-Final.html.

______«The Economy of Ideas», *Wired*, marzo de 1994, p. 129; disponible en http://www.wired.com/wired/archive/2.03/economy.ideas.html.

______«Papers and Comments of a Symposium on Fundamental Rights on the Information Superhighway», *Annual Survey of American Law*, 1994, pp. 355, 358.

BARRY, John M.: *Rising Tide: The Great Mississippi Flood of 1927 and How It Changed America*, Nueva York, Simon and Schuster, 1997.

BARTUSKA, Tom J. y YOUNG, Gerald L. (eds.): *The Built Environment: A Creative Inquiry into Design and Planning*, Menlo Park (Cal.), Crisp Publications, 1994.

BEEN, Vicki: «"Exit" as a Constraint on Land Use Exactions: Rethinking the Unconstitutional Conditions Doctrine», *Columbia Law Review*, núm. 91, 1991, pp. 473-528.

BEESON, Ann y HANSEN, Chris: «Fahrenheit 451.2: Is Cyberspace Burning?», American Civil Liberties Union White Paper, 17 de marzo de 2002.

BELLIA, Patricia L.: «Chasing Bits Across Borders», *University of Chicago Legal Forum*, núm. 35, 2001, p. 100.

BENKLER, Yochai: *The Wealth of Networks: How Social Production Transforms Markets and Freedom,* New Haven, Yale University Press, 2006.

______«Net Regulation: Taking Stock and Looking Forward», *University of Colorado Law Review*, núm. 71, 2000, pp. 1203-1254.

______«Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain», *New York University Law Review*, núm. 74, 1999.

______«Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment», *Harvard Journal of Law and Technology*, núm. 11, 1998, p. 287.

BENOLIEL, Daniel: «Technological Standards, Inc.: Rethinking Cyberspace Regulative Epistemology», *California Law Review*, núm. 92, 2004, p. 1069.

BERMAN, Paul Schiff: «Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation», *University of Colorado Law Review*, núm. 71, 2000, pp. 1263.

BILSTAD, Blake T.: «Obscenity and Indecency in a Digital Age: The Legal and Political Implications of Cybersmut, Virtual Pornography, and the Communications Decency Act of 1996», *Santa Clara Computer and High Technology Law Journal*, núm. 13, 1997, p. 321.

BLACKBURN, David : «On-line Piracy and Recorded Music Sales», Harvard University, Job Market Paper, 2004, disponible en www.katallaxi.se/grejer/blackburn/blackburn_fs.pdf.

BOLE III, Thomas J.: «The Doctrine of Double Effect: Its Philosophical Viability», *Southwest Philosophy Review*, núm. 7, 1991, p. 91.

BORK, Robert H.: *The Antitrust Paradox: A Policy at War with Itself*, Nueva York, Basic Books, 1978.

BOYLE, James: «A Politics of Intellectual Property: Environmentalism for the Net?», *Duke Law Journal*, núm. 47, 1997, p. 87.

______*Shamans, Software, and Spleens: Law and the Construction of the Information Society*, Cambridge (Mass.), Harvard University Press, 1996.

______«Intellectual Property Policy Online», *Harvard Journal of Law and Technology*, vol. 10, núm. 47, 1996, p. 35.

BRACKEN, Paul N. : *The Command and Control of Nuclear Forces*, New Haven, Yale University Press, 1983.

BRADNER, Scott: «The Internet Engineering Task Force», en DiBONA, Chris *et al*. (eds.), *Open Sources: Voices from the Open Source Revolution*, Sebastopol (Cal.), O'Reilly and Associates, 1999.

BRAND, Stewart: *The Media Lab: Inventing the Future at MIT*, Viking Penguin Press, Nueva York, 1987.

BRENNER, Susan: «The Privacy Privilege: Law Enforcement, Technology and the Constitution», *Journal of Technology Law and Policy*, núm. 7, 2002, pp. 123-162.

BREYER, Stephen «The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs», *Harvard Law Review*, núm. 84, 1970.

BRIFFAULT, Richard: «Our Localism: Part I - The Structure of Local Government Law», *Columbia Law Review*, núm. 90, 1990, pp. 1-19.

BRIN, David: *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Boulder, Perseus, 1999.

BRYANT, Meredith Lee: «Combating School Resegregation Through Housing: A Need for a Reconceptualization of American Democracy and the Rights It Protects», *Harvard BlackLetter Journal*, núm. 13, 1997, p. 127.

BUKATMAN, Scott: *Terminal Identity: The Virtual Subject in Postmodern Science Fiction*, Durham (NC), Duke University Press, 1993.

CAIRNCROSS, Frances: *The Death of Distance: How the Communications Revolution Will Change Our Lives*, Boston, Harvard Business School Press, 1997.

CALABRESI, Guido: «The Supreme Court, 1990 Term-Foreword: Antidiscrimination and Constitutional Accountability (Whet the Bork-Brennan Debate Ignores)», Harvard Law Review, núm. 105, 1991, pp. 80-120.

______A Common Law for the Age of Statutes, Cambridge (Mass.), Harvard University Press, 1982.

______y DOUGLAS, A.: «Property Rules, Liability Rules, and Inalienability: One View of the Cathedral», *Harvard Law Review*, núm. 85, 1972, pp. 1089-1106.

CARO, Robert A.: *The Power Broker: Robert Moses and the Fall of New York*, Nueva York, Alfred A. Knopf, 1974.

CARTER, James C.: *The Provinces of the Written and the Unwritten Law*, Nueva York, Banks and Brothers, 1889.

CASTRONOVA, Edward: *Synthetic Worlds: The Business and Culture of Online Games*, Chicago, University of Chicago Press, 2005.

CHANT, Christopher y HOGG, Ian: *The Nuclear War File*, Londres, Ebury Press, 1983.

CLANCY, Thomas K.: «The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures», *University of Memphis Law Review*, núm. 25, 1995, pp. 483-632.

COASE, Ronald H.: «The Problem of Social Cost», *Journal of Law and Economics*, octubre de 1960.

______«The Federal Communications Commission», *Journal of Law and Economics*, núm. 2, 1959.

COHEN, Julie E.: «DRM and Privacy», *Berkeley Technology Law Journal*, núm. 18, 2003, p. 575.

______«Copyright and the Jurisprudence of Self-Help», *Berkeley Technology Law Journal*, núm. 13, 1998, p. 1089.

______«Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"», *Michigan Law Review*, núm. 97, 1998, p. 462.

______«Some Reflections on Copyright Management Systems and Laws Designed to Protect Them», *Berkeley Technology Law Journal*, núm. 12, 1997, pp. 161–182.

______«A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace», *Connecticut Law Review*, núm. 28, 1996.

______«Reverse-Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs», *Southern California Law Review*, núm. 68, 1995, p. 1091.

COJOCARASU, D. I.: *Anti-spam Legislation Between Privacy and Commercial Interest: An Overview of the European Union Legislation Regarding the E-mail Spam*, Oslo, University of Oslo, 2006.

COMMONS, John R.: *Institutional Economics: Its Place in Political Economy*, Edison (NJ), Transaction Publishers, 1990. [New Brunswick (NJ), 1934]

CONWAY, Flo y SIEGELMAN, Jim: *Dark Hero of the Information Age: In Search of Norbert Wiener, The Father of Cybernetics*, Nueva York, Basic Books, 2004.

COOTER, Robert: «Expressive Law and Economics», *Journal of Legal Studies*, núm. 27, 1998, p. 585.

______«Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant», *University of Pennsylvania Law Review*, núm. 144, 1996, pp. 1643-1662.

______«The Theory of Market Modernization of Law», *International Review of Law and Economics*, núm. 16, 1996, p. 141.

CORDELL, Arthur J. *et al*.: *The New Wealth of Nations: Taxing Cyberspace*, Toronto, Between the Lines, 1997.

CRAWFORD, Susan P.: «Someone to Watch Over Me: Social Policies for the Internet», *Cardozo Law School Legal Studies Research Paper*, núm. 129, 2006.

______Symposium «Law and the Information Society, Panel V: Responsibility and Liability on the Internet, Shortness of Vision: Regulatory Ambition in the Digital Age», *Fordham Law Review*, núm. 74, 2005.

CROWLEY, John y MAYER-SCHOENBERGER, Viktor: «Napster's Second Life?—The Regulatory Challenges of Virtual Worlds», Kennedy School of Government, Documento de Trabajo núm. RWP05–052, 2005, p. 8.

CURRIE, David P.: *The Constitution of the Federal Republic of Germany*, Chicago, University of Chicago Press, 1994.

CURTIS, Pavel: «Mudding: Social Phenomena in Text-Based Virtual Realities», en STEFIK, Mark (ed.), *Internet Dreams: Archetypes, Myths, and Metaphors,* Cambridge (Mass.), MIT Press, 1996.

DAKOFF, Howard S.: «The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation», *John Marshall Law Review*, núm. 29, 1996, p. 475.

DAVIDSON, Chandler y GROFMAN, Bernard (eds.): *Quiet Revolution in the South,* Princeton (NJ), Princeton University Press, 1994.

DEMSETZ, Harold: «Toward a Theory of Property Rights», *American Economics Review*, núm. 57, 1967, p. 347.

DEVINS, Neal: *Constitutional Values*, Baltimore, Johns Hopkins University Press, 1996.

DeVOLPI, A. *et al*., *Born Secret: The H-Bomb, The Progressive Case, and National Security*, Nueva York, Pergamon Press, 1981.

DIBBELL, Julian: «Dragon Slayers or Tax Evaders?», *Legal Affairs*, enero/febrero de 2006, p. 47.

______*My Tiny Life: Crime and Passion in a Virtual World*, Londres, Fourth Estate, 1998.

DiBONA, Chris *et al*. (eds.), *Open Sources: Voices from the Open Source Revolution*, Sebastopol (Cal.), O'Reilly and Associates, 1999.

DIFFIE, Whitfield y LANDAU, Susan Eva: *Privacy on the Line: The Politics of Wiretapping and Encryption*, Cambridge (Mass.), MIT Press, 1998.

______y HELLMAN, Martin E.: «New Directions in Cryptography», *IEEE Transactions on Information Theory IT–22*, noviembre de 1976, pp. 29–40.

DI FRANCO *et al*., «Small Vote Manipulations Can Swing Elections», *Communications of the ACM,* vol. 47, núm. 10, 2004, p. 43.

DOHENY-FARINA, Stephen: *The Wired Neighborhood*, New Haven (Conn.), Yale University Press, 1996.

DOWNES, Larry y MUI, Chunka: *Unleashing the Killer App: Digital Strategies for Market Dominance*, Boston, Harvard Business School Press, 1998 [ed. cat.: *Killer app: estratègies digitals per a dominar el mercat,* trad. por Roser Soms Tramujas, Barcelona, Editorial Pòrtic, 2000].

DYSON, Esther: *Release 2.0: A Design for Living in the Digital Age*, Nueva York, Broadway Books, 1997 [ed. cast.: *Realease 2.0*, trad. por Ana Alcaina Pérez, Madrid, Punto de Lectura, 2000].

EASTERBROOK, Frank H.: «Intellectual Property Is Still Property», *Harvard Journal of Law and Public Policy*, núm. 13, 1990, p. 108.

Electronic Frontier Foundation (EFF), *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*, Sebastopol (Cal.), Electronic Frontier Foundation, 1998.

ELKIN-KOREN, Niva: «Contracts in Cyberspace: Rights Without Laws», *Chicago-Kent Law Review*, núm. 73, 1998.

______ «Copyright Policy and the Limits of Freedom of Contract», en *Berkeley Technology Law Journal*, núm. 12, 1997, p. 93.

______«Cyberlaw and Social Change: A Democratic Approach to Copyright Law in Cyberspace», *Cardozo Arts and Entertainment Law Journal*, núm. 14, 1996, p. 215.

______«Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators», *Cardozo Arts and Entertainment Law Journal*, núm. 13, 1995, pp. 345–399.

ELY, John Hart: *Democracy and Distrust: A Theory of Judicial Review*, Cambridge (Mass.), Harvard University Press, 1980 [ed. cast.: *Democracia y desconfianza: una teoría del control constitucional*, trad. por Magdalena Holguín, Santafé de Bogotá, Siglo del Hombre, 1997].

EMERSON, Thomas: «The Doctrine of Prior Restraint», *Law and Contemporary Problems*, núm. 20, 1955, p. 648.

FAGIN, Matthew: «Regulating Speech Across Borders: Technology vs. Values», *Michigan Telecommunications Technology Law Review,* núm. 9, 2003, p. 395.

FAIRFIELD, Joshua A. T.: «Cracks in the Foundation: The New Internet Legislation's Hidden Threat to Privacy and Commerce», *Arizona State Law Journal*, núm. 36, 2004, p. 1193.

FIELD, Richard: «1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States», *American University Law Review*, núm. 46, 1997, pp. 967-993.

FISHER III, William W.: «Property and Contract on the Internet», *Chicago-Kent Law Review*, núm. 74, 1998.

______«Compulsory Terms in Internet-Related Contracts», *Chicago-Kent Law Review*, núm. 73, 1998.

______ *et al*. (eds.), *American Legal Realism,* Nueva York, Oxford University Press, 1993.

______«Reconstructing the Fair Use Doctrine», *Harvard Law Review*, núm. 101, 1988, p. 1659.

FISHKIN, James S.: *The Voice of the People*, New Haven (Conn.), Yale University Press, 1995.

FISS, Owen: *The Irony of Free Speech*, Cambridge (Mass.), Harvard University Press, 1996.

FOOT, Philippa: «The Problem of Abortion and the Doctrine of the Double Effect», en *Virtues and Vices and Other Essays in Moral Philosophy*, Berkeley, University of California Press, 1978 [ed. cast.: *Las virtudes y los vicios y otros ensayos de filosofía moral*, trad. por Claudia Martínez, IIFs-UNAM, México, 1994].

FORD, Daniel: *The Button: The Nuclear Trigger—Does It Work?*, Londres, Allen and Unwin, 1985.

FORD, Richard Thompson: «The Boundaries of Race: Political Geography in Legal Analysis», *Harvard Law Review*, núm. 107, 1994, pp. 1841.

______«Beyond Borders: A Partial Response to Richard Briffault», *Stanford Law Review*, núm. 48, 1996, p. 1173.

______«Geography and Sovereignty: Jurisdictional Formation and Racial Segregation», *Stanford Law Review*, núm. 49, 1997, p. 1365.

FOUCAULT, Michel: *Discipline and Punish: The Birth of the Prison*, Nueva York, Vintage, 1979 [ed. cast.: *Vigilar y castigar: nacimiento de la prisión*, trad. por Aurelio Garzón del Camino, Madrid, Siglo XXI, 1994].

FRANCIA, Peter y HERRNSON, Paul: «The Impact of Public Finance Laws on Fundraising in State Legislative Elections», American Politics Research, v. 31, núm. 5, septiembre de 2003.

FRANKFURTER, Felix: *The Commerce Clause Under Marshall, Taney, and Waite*, Chapel Hill, University of North Carolina Press, 1937.

FREEDMAN, Jonathan L.: *Media Violence and Its Effect on Aggression*, Toronto, Toronto University Press, 2002.

FREIWALD, Susan: «Uncertain Privacy: Communication Attributes After the Digital Telephony Act», *Southern California Law Review*, núm. 69, 1996, p. 949.

FREY, Michael G.: «Unfairly Applying the Fair Use Doctrine: *Princeton University Press vs. Michigan Document Services*, 99 F3d 1381, 6º Cir 1996", *University of Cincinnati Law Review*, núm. 66, 1998, pp. 959-1001.

FRIED, Barbara H.: *The Progressive Assault on Laissez-Faire: Robert Hale and the First Law and Economics Movement*, Cambridge (Mass.), Harvard University Press, 1998.

FRIED, Charles: «Book Review: Perfect Freedom or Perfect Control?», *Harvard Law Review*, núm. 114, 2000, p. 606.

FRISCHMANN, Brett: «Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market», *Columbia Science and Technology Law Review*, núm. 2, 2000/2001, p. 1.

FROOMKIN, Michael: «The Collision of Trademarks, Domain Names, and Due Process in Cyberspace», *Communications of the ACM*, núm. 44, 2001, p. 91.

______«It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow"», *University of Chicago Legal Forum*, 1996, p. 15.

______«The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution», *University of Pennsylvania Law Review*, núm. 143, 1995, pp. 709- 759.

FRUG, Gerald E.: «Universities and Cities», *Connecticut Law Review*, núm. 30, 1998, p. 1199.

FRUG, Jerry:«The Geography of Community», *Stanford Law Review*, núm. 48, 1996, p. 1047.

______ «Decentering Decentralization», *University of Chicago Law Review*, núm. 60, 1993, p. 253.

GANDY, Oscar: *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, Westview Press, 1993.

GARDNER, James A.: «Liberty, Community, and the Constitutional Structure of Political Influence: A Reconsideration of the Right to Vote», *University of Pennsylvania Law Review*, núm. 145, 1997, p. 893.

GAVIT, Bernard C.: *The Commerce Clause of the United States Constitution*, Bloomington (Ind.), Principia Press, 1932.

GEIST, Michael: «Cyberlaw 2.0», *Boston College Law Review*, núm. 44, 2003, p. 323.

______«Is There a There There? Towards Greater Certainty for Internet Jurisdiction», *Berkeley Technology Law Journal*, núm. 16, 2001, p. 1345.

GILLETTE, Clayton P.: *Local Government Law: Cases and Materials*, Boston, Little Brown, 1994.

GINSBURG, Jane C.: «A Tale of Two Copyrights: Literary Property in Revolutionary France and America», *Tulane Law Review*, núm. 64, 1990, p. 991.

GLISSON, Gary W.: «A Practitioner's Defense of the White Paper», *Oregon Law Review*, núm. 75, 1996, p. 277.

GODWIN, Mike: *Cyber Rights: Defending Free Speech in the Digital Age*, Nueva York, Times Books, 1998.

GOLDSMITH, Jack y WU, Timothy: *Who controls the Net? Illusions of a Borderless World*, Nueva York, Oxford University Press, 2006.

______y WU, Timothy: «Digital Borders», *Legal Affairs*, enero /febrero de 2006, p. 44.

______«Against Cyberanarchy», *University of Chicago Law Review*, núm. 65, 1998, p. 1199.

______«The Internet and the Abiding Significance of Territorial Sovereignty», *Indiana Journal of Global Legal Studies*, núm. 5, 1998, p. 475.

GOLDSTEIN, Paul: *Copyright´s Highway: From Gutenberg to the Celestial Jukebox*, Stanford University Press, 2003.

______*Real Property*, Minneola (NY), Foundation Press, 1984.

GOODMAN, Nelson: «How Buildings Mean» en GOODMAN, Nelson y ELGIN, Catherine Z. (eds.): *Reconceptions in Philosophy and Other Arts and Sciences*, Londres, Routledge, 1988.

GORDON, Wendy J.: «Reality as Artifact: From Feist to Fair Use», *Law and Contemporary Problems*, núm. 55, 5PG, 1992, p. 93.

______«On Owning Information: Intellectual Property and Restitutionary Impulse», *Virginia Law Review*, núm. 78, 1992, p. 149.

______«Toward a Jurisprudence of Benefits: The Norms of Copyright and the Problem of Private Censorship», *University of Chicago Law Review*, núm. 57, 1990, p. 1009.

______«An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory», *Stanford Law Review*, núm. 41, 1989, p. 1343.

______«Fair Use as Market Failure», *Columbia Law Review*, núm. 82, 1982.

GRANTHAM, Bill: «America the Menace: France's Feud With Hollywood», *World Policy Journal*, núm. 15, verano de 1998, p. 58.

GREENBERG, Marc H.: «A Return to Lilliput: The LICRA vs. Yahoo! Case and the Regulation of Online Content in the World Market», *Berkeley Technology Law Journal*, núm. 18, 2003, p. 1191.

GUINIER, Lani: «More Democracy», *University of Chicago Legal Forum*, 1995, p. 1.

______*The Tyranny of the Majority: Fundamental Fairness in Representative Democracy*, Nueva York, Free Press, 1994.

GURAK, Laura J.: *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip*, New Haven, Yale University Press, 1997 [de esta autora, en castellano y relacionado: «Las buenas perspectivas y el peligro de la actuación social en el ciberespacio. El *ethos*, la oratoria y las protestas sobre MarketPlace y Clipper chip» en SMITH y KOLLOCK (eds.), *Comunidades en el ciberespacio*, trad. por José María Ruiz Vaca, Barcelona, EDIUOC, 2003].

GUSEWELLE, Charles W. *et al.*: «Round Table Discussion: Violence in the Media», *Kansas Journal of Law and Public Policy*, núm. 4, 1995, p. 39.

HACKETT FISCHER, David: *Albion's Seed: Four British Folkways in America*, Nueva York, Oxford University Press, 1989.

HAFNER, Katie y LYON, Matthew: *Where Wizards Stay Up Late*, Nueva York, Simon and Schuster, 1996.

HAGEL, John y ARMSTRONG, Arthur G.: *Net Gain: Expanding Markets Through Virtual Communities*, Boston, Harvard Business School Press, 1997 [ed. cast.: *Negocios rentables a través de Internet: Net Gain*, trad. por Florentino Heras Díez, Barcelona, Paidós Ibérica, 2000].

HALBERT, Debora J.: *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*, Westport (Conn.), Quorum, 1999.

HALPERIN, Morton H. y HOFFMAN, Daniel N.: *Top Secret: National Security and the Right to Know*, Washington DC, New Republic Books, 1977.

HARDIN, Garrett: «The Tragedy of the Commons», *Science*, 1968 (disponible en http://www.sciencemag.org/cgi/content/full/162/3859/1243).

HARDY, Trotter: «Project Looking Forward: Sketching the Future of Copyright in a NetworkedWorld», informe final de la Oficina de Copyright de EEUU (1998), disponible en http://www.copyright.gov/reports/thardy.pdf.

HARFST, Gerold (ed.), *German Criminal Law,* vol. 1, Würzburg, Harfst Verlag, 1989 [ed. cast: Emilio Eiranova Encinas (coord.), *Código Penal Alemán StGB, Código Procesal Penal Alemán StPO*, trad. por Juan Ortiz de Noriega, Madrid, Marcial Pons, 2000].

HART, H. L. A.: *The Concept of Law* (2ª), Nueva York, Oxford University Press, 1994 [ed. cast: *El concepto de Derecho*, trad. por Genaro R. Carrio Buenos Aires, Abeledo-Perrot, 1990].

HASEN, Richard L.: «Symposium: Law, Economics, and Norms: Voting Without Law?», *University of Pennsylvania Law Review*, núm. 144, 1996, p. 2135.

HAYNES, Mark: «Black Holes of Innovation in the Software Arts», *Berkeley Technology Law Journal*, núm. 14, 1999, p. 503.

HAZLETT, Thomas W.: «Physical Scarcity, Rent Seeking, and the First Amendment», *Columbia Law Review*, núm. 97, 1997, pp. 905–934.

______«The Rationality of U.S. Regulation of the Broadcast Spectrum», *Journal of Law and Economics*, núm. 33, 1990, p. 133.

HEALY, Margaret A.: «Prosecuting Child Sex Tourists at Home: Do Laws in Sweden, Australia, and the United States Safeguard the Rights of Children as Mandated by International Law?», *Fordham International Law Journal*, núm. 18, 1995, pp. 1852-1912.

HEFFAN, Ira V.: «Copyleft: Licensing Collaborative Works in the Digital Age», *Stanford Law Review*, núm. 49, 1997, p. 1487.

HELLER, Michael A.: «The Tragedy of the Anticommons: Property in the Transition from Marx to Markets», *Harvard Law Review*, núm. 111, 1998, p. 621.

HELLMAN, Deborah: «The Importance of Appearing Principled», Arizona Law Review, núm. 37, 1995, p. 1107.

HELMS, Shawn C.: «Translating Privacy Values with Technology», *Boston University Journal of Science and Technology Law*, núm. 7, 2001, pp. 288-314.

HELPER, Rose: *Racial Policies and Practices of Real Estate Brokers*, Minneapolis, University of Minnesota Press, 1969.

HERZ, J. C.: *Surfing on the Internet: A Nethead's Adventures On-Line*, Boston, Little Brown, 1995.

HETCHER, Steven A.: «Norm Proselytizers Create a Privacy Entitlement in Cyberspace», *Berkeley Technology Law Journal*, núm. 16, 2001, p. 877.

HIGGINBOTHAM Jr., A. Leon: «Racism in American and South African Courts: Similarities and Differences», *New York University Law Review*, núm. 65, 1990, p. 479.

HOLETON, Richard (ed.): *Composing Cyberspace: Identity, Community, and Knowledge in the Electronic Age*, Boston, McGraw-Hill, 1998.

HOLMES, Oliver Wendell Jr., «The Path of the Law», *Harvard Law Review*, núm. 10, 1897, p. 457.

HORN, Stacy: *Cyberville: Clicks, Culture, and the Creation of an Online Town*, Nueva York, Warner Books, 1998.

HOVENKAMP, Herbert: *Enterprise and American Law, 1836–1937*, Cambridge (Mass.), Harvard University Press, 1991.

HUBER, Peter: *Law and Disorder in Cyberspace: Abolish the FCC and Let Common Law Rule the Telecosm*, Nueva York, Oxford University Press, 1997.

______*Orwell's Revenge: The 1984 Palimpsest*, Nueva York, Maxwell Macmillan International, 1994.

HUGHES, Eric: «A Cypherpunk's Manifesto», en SCHNEIER, Bruce (ed.): *Applied Cryptography,* (2ª), Nueva York, Wiley, 1996, p. 609 [ed. cast.: «Un Manifiesto Cripto-hacker» en Carlos Gradin (comp.), *Internet, hackers y software libre*, Buenos Aires, Editora Fantasma, 2004, pp. 95-99; disponible en www.dyne.org/editora_fantasma.pdf].

HUNT, Craig: *TCP/IP Network Administration* (2ª), Sebastopol (Cal.), O'Reilly and Associates, 1998.

HUNTER, Dan y LASTOWKA, F. Gregory: «Amateur-to-Amateur», *William and Mary Law Review*, núm. 46, diciembre de 2004, pp. 951-1027.

______«Cyberspace as Place and the Tragedy of the Digital Anti-commons», *California Law Review*, núm. 91, 2003, p. 439.

______«Philippic.com», *California Law Review*, núm. 90, 2002, p. 611.

IRONS, Peter y GUITTON, Stephanie (eds.): *May It Please the Court: The Most Significant Oral Arguments Made Before the Supreme Court Since 1955,* Nueva York, Free Press, 1993.

JACKSON, Kenneth T.: *Crabgrass Frontier: the Suburbanization of the United States*, Nueva York, Oxford University Press, 1985.

JAEGER, Walter H. E. (ed.): *Williston on Contracts* (3ª), Mount Kisco (NY), Baker Voorhis, 1957.

JASZI, Peter A.: «Goodbye to All That—A Reluctant (and Perhaps Premature) Adieu to a Constitutionally Grounded Discourse of Public Interest in Copyright Law», *Vanderbilt Journal of Transnational Law*, núm. 29, 1996, p. 595.

______«On the Author Effect: Contemporary Copyright and Collective Creativity», *Cardozo Arts and Entertainment Law Journal*, núm. 10, 1992, pp. 293-320.

______«Toward a Theory of Copyright: The Metamorphoses of "Authorship"», *Duke Law Journal* 1991, p. 455.

JEFFERSON, Thomas: «Carta a Isaac Mcpherson, 13 de agosto de 1813», reimpresa en WASHINGTON, H. A. (ed.): *Writings of Thomas Jefferson, 1790–1826,* vol. 6, Washington DC, Taylor & Matjry, 1854, pp. 180–181.

JOHNSON, David R. y POST, David: «Law and Borders—The Rise of Law in Cyberspace», *Stanford Law Review*, núm. 48, 1996, p. 1367.

______y MARKS, Kevin A.: «Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?», *Villanova Law Review*, núm. 38, 1993, p. 487.

JOHNSON, Steven: *Interface Culture: How New Technology Transforms the Way We Create and Communicate*, San Francisco, Harper Edge, 1997.

JOHNSTON, David; HANDA, Sunny; y MORGAN, Charles: *Cyberlaw: What You Need to Know About Doing Business Online*, Toronto, Stoddart, 1997.

JOLLY, Adam and PHILPOTT, Jeremy (eds.): *A Handbook of Intellectual Property Management: Protecting, Developing and Exploiting Your IP Assets*, Londres, Kogan Page, 2004.

KAHAN, Dan M.: «Punishment Incommensurability», *Buffalo Criminal Law Review*, núm. 1, 1998, p. 691.

______«Ignorance of Law Is an Excuse—But Only for the Virtuous», *Michigan Law Review*, núm. 96, 1997, p. 127.

KAHIN, Brian y VARIAN, Hal R. (eds.): *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*, Cambridge (Mass.), MIT Press, 2000.

KAMM, Frances M.: «The Doctrine of Double Effect: Reflections on Theoretical and Practical Issues», *Journal of Medicine and Philosophy*, núm. 16, 1991, p. 571.

KAPLAN, Benjamin: *An Unhurried View of Copyright*, Nueva York, Columbia University Press, 1967.

KATSH, Ethan: «Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace», *University of Chicago Legal Forum*, 1996, p. 335.

KATYAL, Neal Kumar: «Architecture as Crime Control», *Yale Law Journal*, núm. 111, 2002, p. 1039.

KATYAL, Sonia K.: «The New Surveillance», *Case Western Reserve Law Review*, núm. 54, 2003, p. 297.

KATZ, Peter: *The New Urbanism: Toward an Architecture of Community*, Nueva York, McGraw-Hill, 1994.

KELLEY, Kevin: *Out of Control: The New Biology of Machines, Social Systems and the Economic World*, Reading (Mass.), Addison-Wesley, 1994.

KENDALL, Lori: «MUDder? I Hardly Know 'Er!: Adventures of a Feminist MUDder», en CHERNY, Lynn y WEISE, Elizabeth Reba (eds.): *Wired Women: Gender and New Realities in Cyberspace*, Seattle, Seal Press, 1996.

KENNEDY, John F.: *Profiles in Courage*, Nueva York, Harper, 1956 [ed. cast.: *Perfiles de Coraje*, trad por. Francisco Bermeosolo, Buenos Aires, Plaza & Janes, 1964].

KENNETH J. Arrow, «Economic Welfare and the Allocation of Resources for Invention», en *The Rate and Direction of Inventive Activity: Economic and Social Factors*, Princeton (NJ), Princeton University Press, 1962.

KENWOOD, Carolyn A. *A Business Case Study of Open Source Software*, Mitre Corporation, 2001.

KERR, Orin: «The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution», *Michigan Law Review*, núm. 102, marzo de 2004, p. 801.

KESAN, Jay P. y SHAH, Rajiv C.: «Shaping Code», *Harvard Journal of Law and Technology*, núm. 18, 2005, pp. 319–338.

______y GALLO, Andres A.: «Optimizing Regulation of Electronic Commerce», *University of Cincinnati Law Review*, núm. 72, 2004, p. 1497.

______«Private Internet Governance», *Loyola University Chicago Law Journal*, núm. 35, 2003, p. 87.

KOSMAN, Joel: «Toward an Inclusionary Jurisprudence: A Reconceptualization of Zoning», *Catholic University Law Review*, núm. 43, 1993, pp. 59-103.

KROL, Ed: *The Whole Internet: User's Guide and Catalogue*, Sebastopol (Cal.), O'Reilly and Associates, 1992.

KURLAND, Philip B. y CASPER, Gerhard (eds.): *Fifty-four Landmark Briefs and Arguments of the Supreme Court of the United States: Constitutional Law*, Washington DC, University Publications of America, 1975.

LANDES, William M. y POSNER, Richard A.: *The Economic Structure of Intellectual Property Law*, Cambridge, Mass., Harvard University Press, 2003.

______«An Economic Analysis of Copyright Law», *Journal of Legal Studies*, núm. 18, 1989, pp. 325–46.

LANE, Thomas A.: «Of Hammers and Saws: The Toolbox of Federalism and Sources of Law for the Web», *New Mexico Law Review*, núm. 33, 2003, p. 115.

LANGE, David: «Recognizing the Public Domain», *Law and Contemporary Problems*, núm. 44, 1981, p. 147.

LASICA, J. D.: *Darknet: Hollywood's War Against the Digital Generation*, Nueva York, Wiley, 2005 [ed. cast.: *Darknet: la guerra contra la generación digital y el futuro de los medios audiovisuales*, trad. por María Lourdes Silveira Lanot, Madrid, Editorial Nowtilus, 2006].

LASTOWKA, Gregory y Hunter, Dan: «The Laws of Virtual Worlds», *California Law Review*, núm. 92, 2004, pp. 1-73.

LAUGHLIN, Gregory K.: «Sex, Lies, and Library Cards: The First Amendment Implications of the Use of Software Filters to Control Access to Internet Pornography in Public Libraries», *Drake Law Review*, núm. 51, 2003, pp. 213–268.

LEHMAN, Bruce: intervención previa al «Congreso Inagural Engelberg sobre Cultura y Economía de Participación en un Régimen de Propiedad Intelectual Internacional», *New York University Journal of International Law and Politics*, núm. 29, 1996–97, p. 211.

LEMLEY, Mark A.: «Place and Cyberspace», *California Law Review*, núm. 91, 2003, p. 521.

______«Private Property», *Stanford Law Review*, núm. 52, 2000, p. 1545.

______«Beyond Preemption: The Law and Policy of Intellectual Property Licensing», *California Law Review*, núm. 111, 1999.

______«The Economics of Improvement in Intellectual Property Law», *Texas Law Review*, núm. 75, 1997, pp. 989–1068.

______y O'BRIEN, David W.: «Encouraging Software Reuse», *Stanford Law Review*, núm. 49, 1997, p. 255.

______«Romantic Authorship and the Rhetoric of Property», *Texas Law Review*, núm. 75, 1997, p. 873.

______«Intellectual Property and Shrink-wrap Licenses», *Southern California Law Review*, núm. 68, 1995, pp. 1239.

LENNERTZ, William: «Town-Making Fundamentals», en DUANY, Andres y PLATER-ZYBERK , Elizabeth (eds.): *Towns and Town-Making Principles*, Nueva York, Rizzoli, 1991.

LESSIG, Lawrence: «On the Internet and the Benign Invasions of Nineteen Eighty-Four», en GLEASON, Abbott, GOLDSMITH, Jack y NUSSBAUM, Martha C. (eds.): *On «Nineteen Eighty-Four»: Orwell and Our Future*, Princeton, Princeton University Press, 2005.

__________*Free Culture: The Nature and Future of Creativity*, Nueva York, The Penguin Press, 2004 [ed. cast.: *Por una cultura libre*, Madrid, Traficantes de Sueños, 2005].

______*The Future of Ideas: The Fate of the Commons in a Connected World*, Nueva York, Random House, 2001.

______«The New Chicago School», *Journal of Legal Studies*, núm. 27, 1998, p. 661.

______«Fidelity and Constraint», *Fordham Law Review*, núm. 65, 1997, p. 1365.

______«Reading the Constitution in Cyberspace», *Emory Law Journal*, núm. 45, 1996, p. 869.

______«The Regulation of Social Meaning», *The University of Chicago Law Review*, vol. 62, núm. 3, 1995, pp. 943-1045.

______«Translating Federalism: United States vs. Lopez», *Supreme Court Review*, 1995, p. 125.

______«Fidelity in Translation», *Texas Law Review*, núm. 71, 1993, pp. 1165-1230.

LEVY, Steven: *Hackers: Heroes of the Computer Revolution*, Garden City (NY), Anchor Press/Doubleday, 1984.

LITMAN, Jessica: «The Tales That Article 2B Tells», *Berkeley Technology Law Journal*, núm. 13, 1998, p. 931.

______«Reforming Information Law in Copyright's Image», *Dayton Law Review*, núm. 22, 1997, p. 587.

______«Revising Copyright Law for the Information Age», *Oregon Law Review*, núm. 75, 1996, p. 19.

______«The Exclusive Right to Read», *Cardozo Arts and Entertainment Law Journal*, núm. 13, 1994, p. 29.

______«Copyright as Myth», *University of Pittsburgh Law Review*, núm. 53, 1991, p. 235.

______«The Public Domain», *Emory Law Journal*, núm. 39, 1990, p. 965.

LODER, Theodore, VAN ALSTYNE, Marshall y WASH, Rick: «An Economic Response to Unsolicited Communication», *Advances in Economic Analysis and Policy*, vol. 6, núm. 1, art. 2, 2006, disponible en http://www.bepress.com/bejeap/advances/vol6/iss1/art2.

LONG, Herman H. y JOHNSON, Charles S.: *People Versus Property: Race-Restrictive Covenants in Housing*, Nashville, Fisk University Press, 1947.

LOSHIN, Peter: *TCP/IP Clearly Explained*, San Francisco, Morgan Kaufmann, 1997.

MACLIN, Tracey: «The Complexity of the Fourth Amendment: A Historical Review», *Boston University Law Review*, núm. 77, 1997, p. 925.

MADISON, Michael J.: «Rights of Access and the Shape of the Internet», *Boston College Law Review*, núm. 44, 2003, p. 433.

MANGABEIRA UNGER, Roberto: *Social Theory: Its situation and Its Task*, Nueva York, Cambridge University Press, 1987.

______*Social Theory Politics: A Work in Constructive Social Theory,* v. II, Nueva York, Cambridge University Press, 1987.

MASSEY, Douglas S. y DENTON, Nancy A.: *American Apartheid: Segregation and the Making of the Under Class*, Cambridge (Mass.), Harvard University Press, 1993.

MAYER-SCHONBERGER, Viktor y FOSTER, Teree E.: «A Regulatory Web: Free Speech and the Global Information Infrastructure», *Michigan Telecommunications and Technology Law Review,* vol. 3, núm. 45, 1997.

McGEVERAN, William: «Programmed Privacy Promises: P3P and Web Privacy Law», *New York University Law Review*, núm. 76, 2001, p. 1813.

McGOWAN, David: «Legal Implications of Open Source Software», *Illinois University Law Review*, núm. 241, 2001.

McJOHN, Stephen M.: «The Paradoxes of Free Software», *George Mason Law Review*, núm. 9, 2000, pp. 25-65.

______«Fair Use and Privatization in Copyright», *San Diego Law Review*, núm. 35, 1998, p. 61.

McTAGGART, Craig: «A Layered Approach to Internet Legal Analysis», *McGill Law Journal*, núm. 48, 2003, p. 571.

MEARES, Tracey L.: «Social Organization and Drug Law Enforcement», *American Criminal Law Review*, núm. 35, 1998, p. 191.

______«Charting Race and Class Differences in Attitudes Toward Drug Legalization and Law Enforcement: Lessons for Federal Criminal Law», *Buffalo Criminal Law Review*, núm. 1, 1997, p. 137.

MERGES, Robert P. *et al.*: *Intellectual Property in the New Technological Age*, Nueva York, Aspen Law and Business, 1997.

MINOW, Martha: *Making All the Difference: Inclusion, Exclusion, and American Law*, Ithaca (NY), Cornell University Press, 1990.

MITCHELL, William J.: *City of Bits: Space, Place, and the Infobahn*, Cambridge (Mass.), MIT Press, 1995.

MNOOKIN, Jennifer: «Virtual(ly) Law: The Emergence of Law on LambdaMOO», *Journal of Computer-Mediated Communication*, núm. 2, 1996.

MOGLEN, Eben: «The Invisible Barbecue», *Columbia Law Review*, núm. 97, 1997, p. 945.

MONCHAUX, John de y SCHUSTER, J. Mark: «Five Things to Do», en SCHUSTER (ed.): *Preserving the Built Heritage*, Hanover (NH), University Press of New England, 1997.

MONTPAS, Scott M.: «Gambling Online: For a Hundred Dollars, I Bet You Govern ment Regulation Will Not Stop the Newest Form of Gambling», *University of Dayton Law Review*, núm. 22, 1996, p. 163.

MORLAND, Howard: *The Secret That Exploded*, Nueva York, Random House, 1981.

MURPHY, Sandi R.:«Drug Diplomacy and the Supply-Side Strategy: A Survey of United States Practice», *Vanderbilt Law Review*, núm. 43, 1990, p. 1259.

NACHBAR, Thomas B.: «Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character», *Minnesota Law Review*, núm. 85, 2000, p. 215.

NADER, Ralph: *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*, Nueva York, Grossman, 1965.

NEGROPONTE, Nicholas: *Being Digital*, Nueva York, Alfred A. Knopf, 1995 [ed. cast.: *El mundo digital*, trad. por Marisa Aboala, Barcelona, Ediciones B, 1999].

NELSON, Janai S.: «Residential Zoning Regulations and the Perpetuation of Apartheid», *UCLA Law Review*, núm. 43, 1996, p. 1689.

NETANEL, Neil Weinstock: «Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory», *California Law Review*, núm. 88, 2000, p. 395.

______«Asserting Copyright's Democratic Principles in the Global Arena», *Vanderbilt Law Review*, núm. 51, 1998, pp. 217-299.

______«[C]opyright and a Democratic Civil Society», *Yale Law Journal*, núm. 106, 1996, pp. 283–336.

______«Alienability Restrictions and the Enhancement of Author Autonomy in United States and Continental Copyright Law», *Cardozo Arts and Entertainment Law Journal*, núm. 12, 1994, pp. 1–43.

NGUYEN, Alexander T.: «Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked The Fourth Amendment?», *Virginia Journal of Law and Technology*, núm. 7, 2002.

NISSENBAUM, Helen: «Securing Trust Online: Wisdom or Oxymoron», *Boston University Law Review*, núm. 81, 2001, p. 635.

______«Values in the Design of Computer Systems», *Computers and Society*, marzo de 1998, p. 38.

NOAM, Eli: «Spectrum Auctions: Yesterday's Heresy, Today's Orthodoxy, Tomorrow's Anachronism —Taking the Next Step to Open Spectrum Access», *Journal of Law and Economics*, núm. 41, 1998, p. 765.

NOVECK, Simone Beth: «Designing Deliberative Democracy in Cyberspace: The Role of the Cyber-Lawyer», *Boston University Journal of Science and Technology Law*, núm. 9, 2003.

NUNZIATO, Dawn C.: «The Death of the Public Forum in Cyberspace», *Berkeley Technology Law Journal*, núm. 20, 2005, pp. 1115-1170.

OLSON, Trisha: «The Natural Law Foundation of the Privileges or Immunities Clause of the Fourteenth Amendment», *Arkansas Law Review*, núm. 48, 1995, p. 347.

ORDOVER, Janusz A. *et al*.: «Predatory Systems Rivalry: A Reply», *Columbia Law Review*, núm. 83, 1983, p. 1150.

O'ROURKE, Maureen «Fencing Cyberspace: Drawing Borders in a Virtual World», *Minnesota Law Review*, núm. 82, 1998.

PERENS, Bruce: «The Open Source Definition», en DiBONA *et al*. (eds.), *Open Sources. Voices from the Open Source Revolution*, Sebastopol (Cal.), O'Reilly and Associates, 1999.

PERRITT, Henry H. Jr.: «Towards a Hybrid Regulatory Scheme for the Internet», *University of Chicago Legal Forum*, núm. 215, 2001.

______«Cyberspace Self-government: Town Hall Democracy or Rediscovered Royalism?», *Berkeley Technology Law Journal*, núm. 12, 1997, p. 413.

PETERS, Christopher J. y DEVINS, Neal: «Alexander Bickel and the New Judicial Minimalism», en WARD, Kenneth D. y CASTILLO, Cecilia R. (eds.): *The Judiciary and American Democracy*, Albany, State University of New York Press, 2005.

PLATÓN: *Plato's Republic, Book II*, Agoura Publications, Inc., 2001 [ed. cast.: *La República*, trad. por Manuel Fernández-Galiano y José Manuel Pabón y Suárez de Urbina, Madrid, Centro de Estudios Constitucionales, 1970].

PLESSIS, Alain: *The Rise and Fall of the Second Empire, 1852–1871*, Nueva York, Cambridge University Press, 1985.

POOL, Ithiel de Sola: *Technologies Without Boundaries: On Telecommunications in a Global Age*, Cambridge (Mass.), Harvard University Press, 1990.

POSNER, Eric A.: «The Regulation of Groups: The Influence of Legal and Nonlegal Sanctions on Collective Action», *University of Chicago Law Review*, núm. 63, 1996, p. 133.

POSNER, Richard: *Law and Literature*, Cambridge (Mass.), Harvard University Press, 1998 [ed. cast.: *Ley y literatura*, trad. por Pilar Salamanca, Valladolid, Cuatro y el Gato 2004].

______«The Cost of Rights: Implications for Central and Eastern Europe—and for the United States», *Tulsa Law Journal*, núm. 32, 1996.

______*The Problems of Jurisprudence*, Cambridge (Mass.), Harvard University Press, 1990.

POST, David G.: «The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed», *Indiana Journal of Global Legal Studies*, núm. 5, 1998, p. 521.

______«Governing Cyberspace», *Wayne Law Review*, núm. 43, 1996, p. 155.

______«The New Electronic Federalism», *American Lawyer*, octubre de 1996, p. 93.

______«Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace», *Journal of Online Law*, 1995, artículo 3, disponible en http://www.wm.edu/law/publications/jol/articles/post.shtml.

POST, Robert C.: *Constitutional Domains: Democracy, Community, Management*, Cambridge (Mass.), Harvard University Press, 1995.

POWE Jr., L. A.: «The H-Bomb Injunction», *University of Colorado Law Review*, núm. 61, 1990, p. 55.

PRICE, Monroe E. y DUFFY, John F.: «Technological Change and Doctrinal Persistence: Telecommunications Reformin Congress and the Court», *Columbia Law Review*, núm. 97, 1997, p. 976.

QUINN, Warren: «Actions, Intentions, and Consequences: The Doctrine of Double Effect», *Philosophy and Public Affairs*, núm. 18, 1989, p. 334.

RADIN, Margaret Jane y WAGNER, Polk «The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace», *Chicago-Kent Law Review*, núm. 73, 1998.

______*Reinterpreting Property*, Chicago, University of Chicago Press, 1993.

RAKOVE, Jack N.: *Original Meanings: Politics and Ideas in the Making of the Constitution*, Nueva York, Alfred A. Knopf, 1996.

REED Powell, Thomas: «The Child Labor Law, the Tenth Amendment, and the Commerce Clause», *Southern Law Quarterly*, núm. 3, 1918, pp. 175–201.

REID, Elizabeth: «Hierarchy and Power: Social Control in Cyberspace», en SMITH y KOLLOCK (eds.): *Communities in Cyberspace*, Nueva York, Routledge, 1999 [ed. cast.: *Comunidades en el ciberespacio*, trad. por José María Ruiz Vaca, Barcelona, EDIOUC, 2003].

REIDENBERG, Joel R.: «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, núm. 153, 2005, p. 1951.

______«Lex Informatica: The Formulation of Information Policy Rules Through Technology», *Texas Law Review*, núm. 76, 1998, p. 553.

______«Governing Networks and Rule-Making in Cyberspace», *Emory Law Journal*, núm. 45, 1996, p. 911.

RESNICK, Paul: «Filtering Information on the Internet», *Scientific American*, núm. 106, marzo de 1997, también disponible en http://chinese-school.netfirms.com/Internet-filtering.html.

RHEINGOLD, Howard: *The Virtual Community: Homesteading on the Electronic Frontier*, Reading (Mass.), Addison-Wesley, 1993 [ed. cast.: *La comunidad virtual: una sociedad sin fronteras*, trad. por José Ángel Álvarez, Barcelona, Gedisa, 1996].

RICHARDS, Neil M.: «Reconciling Data Privacy and the First Amendment» *UCLA Law Review*, núm. 52, 2005, p. 1148.

RIMM, Marty: «Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in over 2,000 Cities in Forty Countries, Provinces, and Territories», *Georgetown University Law Journal*, núm. 83, 1995, p. 1849.

ROGERS, John: «Bombs, Borders, and Boarding: Combatting International Terrorism at United States Airports and the Fourth Amendment», *Suffolk Transnational Law Review*, núm. 20, 1997, p. 501.

ROSE, Carol M.: «The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems», *Minnesota Law Review*, núm. 83, 1998, p. 129.

______«The Comedy of the Commons: Commerce, Custom and Inherently Public Property», *University of Chicago Law Review*, núm. 53, 1986, pp. 711-781.

ROSEN, Jeffrey: *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, Nueva York, Random House, 2004.

ROTENBERG, Marc: «Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)», *Stanford Technology Law Review*, 2001, pp. 1-90.

ROTFELD, Herbert J. *et al.*, «Television Station Standards for Acceptable Advertising», *Journal of Consumer Affairs*, núm. 24, 1990, p. 392.

RUBENFELD, Jed: *Freedom and Time: A Theory of Constitutional Government*, New Haven, Yale University Press, 2001.

______«On Fidelity in Constitutional Law», *Fordham Law Review*, núm. 65, 1997, p. 1469.

______«Reading the Constitution as Spoken», *Yale Law Journal*, núm. 104, 1995, p. 1119.

RUDENSTINE, David: *The Day the Presses Stopped: A History of the Pentagon Papers Case*, Berkeley, University of California Press, 1996.

SALTZER, Jerome H. *et al.*: «End-to-End Arguments in System Design», en BHARGAVA, Amit (ed.): *Integrated Broadband Networks*, Norwood (Mass.), Artech House, 1991.

SAMUELSON, Pamela: «Encoding the Law into Digital Libraries», *Communications of the ACM*, núm. 41, 1999, p. 13.

______prólogo a «Symposium: Intellectual Property and Contract Law for the Information Age», *California Law Review*, núm. 87, 1998.

______«Embedding Technical Self-Help in Licensed Software», *Communications of the ACM*, núm. 40, 1997, p. 13.

______y REICHMAN, J. H.: «Intellectual Property Rights in Data?», *Vanderbilt Law Review*, núm. 50, 1997, pp. 51–95.

______«The Copyright Grab», *Wired*, enero de 1996, p. 134.

______*et al.*: «A Manifesto Concerning the Legal Protection of Computer Programs», *Columbia Law Review*, núm. 94, 1994, p. 2308.

______«Fair Use for Computer Programs and Other Copyrightable Works in Digital Form: The Implications of Sony, Galoob and Sega», *Journal of Intellectual Property Law*, núm. 1, 1993, p. 49.

SANDERS, James: *The Downing of TWA Flight 800*, Nueva York, Kensington Publishing, 1997.

SCHAUER, Frederick: «Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect"», *Boston University Law Review*, núm. 58, 1978, pp. 685–730.

SCHEURER, Kirsten: «The Clipper Chip: Cryptography Technology and the Constitution», *Rutgers Computer and Technology Law Journal*, núm. 21, 1995, p. 263.

SCHLEGEL, John Henry: *American Legal Realism and Empirical Social Science*, Chapel Hill, University of North Carolina Press, 1995.

SCHNEIDER, Fred B. (ed.): *Trust in Cyberspace*, Washington DC, National Academy Press, 1999.

SCHNEIER, Bruce: *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* (2ª), Nueva York, Wiley, 1996.

SCHULTZ, Thomas: «Does Online Dispute Resolution Need Governmental Intervention? The Case for Architectures of Control and Trust», *North Carolina Journal of Law and Technology*, núm. 6, 2004, p. 71.

SCHUSTER, Mark *et al*. (eds.): *Preserving the Built Heritage: Tools for Implementation*, Hanover (NH), University Press of New England, 1997.

SCHWARTZ, Paul M.: «Beyond Lessig's Code for Internet Privacy: Cyberspace Filter, Privacy Control, and Fair Information Practices», *Wisconsin Law Review*, 2000, p. 743.

SHAPIRO, Andrew: «The "Principles in Context" Approach to Internet Policymaking», *Columbia Science and Technology Law Review*, núm. 1, 2000.

______*The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, Nueva York, PublicAffairs, 1999 [ed. cast.: *El mundo en un clic: cómo Internet pone el control en sus manos (y está cambiando el mundo que conocemos)* trad. por Francisco J. Ramos Mena, Barcelona, Grijalbo Mondadori, 2001].

SHAPIRO, Carl: «Will Ecommerce Erode Liberty?», *Harvard Business Review*, mayo-junio de 2000, p. 195.

SHENK, David: *Data Smog: Surviving the Information Glut*, San Francisco, Harper Edge, 1997.

SHIFFRIN, Steven H.: *The First Amendment, Democracy, and Romance*, Cambridge (Mass.), Harvard University Press, 1990.

SHKLAR, Judith N.: *American Citizenship: The Quest for Inclusion*, Cambridge (Mass.), Harvard University Press, 1991.

SHULMAN, Seth: *Owning the Future*, Boston, Houghton Mifflin, 1999.

SIDAK, Joseph Gregory: «Debunking Predatory Innovation», *Columbia Law Review*, núm. 83, 1983, p. 1121.

SILBERMAN, Steve: «We're Teen, We're Queer, and We've Got E-Mail», *Wired*, noviembre de 1994, pp. 76-80, reeditado en HOLETON, Richard (ed.): *Composing Cyberspace: Identity, Community, and Knowledge in the Electronic Age*, Boston, McGraw-Hill, 1998.

SMIRNOFF III, George: «Copyright on the Internet: A Critique of the White Paper's Recommendation for Updating the Copyright Act and How the Courts Are Already Filling in Its Most Important Shortcoming, Online Service Provider Liability», *Cleveland State Law Review*, núm. 44, 1996.

SMITH, Harold: «Property in Cyberspace», *University of Chicago Law Review*, núm. 63, 1996.

SMITH, James Morton: *Freedom's Fetters: The Alien and Sedition Laws and American Civil Liberties*, Ithaca (NY), Cornell University Press, 1956.

SMITH, Marc A. y KOLLOCK, Peter: *Communities in Cyberspace*, Nueva York, Routledge, 1999 [ed. cast.: *Comunidades en el ciberespacio*, trad. por José María Ruiz Vaca, Barcelona, EDIUOC, 2003].

SMITH, Marlin H.: «The Limits of Copyright: Property, Parody, and the Public Domain», *Duke Law Journal*, núm. 42, 1993, pp. 1233-1272.

SMITH, Merritt Roe y MARX, Leo (eds.): *Does Technology Drive History?: The Dilemma of Technological Determinism*, Cambridge, MIT Press, 1994 [ed. cast.: *Historia y determinismo tecnológico*, trad. por Esther Rabasco Espáriz y Luis Toharia Cortés, Madrid, Alianza Editorial, 1996].

SMITH, Richard: *Internet Cryptography*, Boston, Addison-Wesley, 1997.

SOLOVE, Daniel J., ROTENBERG, Marc y SCHWARTZ, Paul M.: *Information Privacy Law*, (2ª), Nueva York, Aspen Publishers, 2006.

SOLUM, Lawrence B. y CHUNG, Minn: «The Layers Principle: Internet Architecture and the Law», *Public Law and Legal Theory*, Universidad de San Diego, informe de investigación núm. 55, disponible en http://ssrn.com/abstract=416263.

SORKIN, Michael: *Local Code: The Constitution of a City at 42N Latitude*, Nueva York, Princeton Architectural Press, 1993.

SPAINHOWER, Rebecca: *«Virtually Inevitable»: Real Problems in Virtual Communities*, Evanston (Illinois), Northwestern University Press, 1994.

SPAMMER-X, POLSUNS, Jeffrey y SJOUWERMAN, Stu: *Inside the Spam Cartel: Trade Secrets from the Dark Side*, Nueva York, Syngress Publishing, 2004.

SPENCER, Henry y LAWRENCE, David: *Managing USENET*, Sebastopol (Cal.), O'Reilly and Associates, 1998.

STARR, Paul: *The Creation of Media: Political Origins of Modern Communications*, Nueva York, Basic Books, 2004.

STEFIK, Mark: *The Internet Edge: Social, Technical, and Legal Challenges for a Networked World*, Cambridge, MIT Press, 1999.

______«Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing», *Berkeley Technology Law Journal*, núm. 12, 1997, p. 137.

______«Trusted Systems», *Scientific American*, marzo de 1997, p. 78.

______«Letting Loose the Light: Igniting Commerce in Electronic Publication» y «Epilogue: Choices and Dreams», en STEFIK, Mark (ed.), *Internet Dreams: Archetypes, Myths, and Metaphors*, Cambridge (Mass.), MIT Press, 1996.

STEIKER, Carol S.: «Second Thoughts About First Principles», *Harvard Law Review*, núm. 107, 1994, p. 820.

STEIN, Allan R.: «The Unexceptional Problem of Jurisdiction in Cyberspace», *The International Lawyer*, núm. 32, 1998, p. 1167.

STEPHENSON, Neal: *Snow Crash*, Nueva York, Bantam, 1992 [ed. cast.: *Snow Crash*, trad. por Juan Manuel Barranquero Ríos, Barcelona, Gigamesh, 2005].

STONE, Geoffrey: «Imagining a Free Press», *Michigan Law Review*, núm. 90, 1992, pp. 1246-1264.

STRAHILEVITZ, Lior Jacob: «A Social Networks Theory of Privacy», *University of Chicago Law Review*, núm. 72, 2005, p. 919.

______«Charismatic Code, Social Norms and the Emergence of Cooperation on the File-Swapping Networks», *Virginia Law Review*, núm. 89, 2003, p. 505.

STRASSER, Mathias: «A New Paradigm in Intellectual Property Law? The Case Against Open Sources», *Stanford Technology Law Journal*, 2001.

STUNTZ, William J.: «The Uneasy Relationship Between Criminal Procedure and Criminal Justice», *Yale Law Journal*, núm. 107, 1997.

______«Privacy's Problem and the Law of Criminal Procedure», *Michigan Law Review*, núm. 93, 1995, p. 1016.

______«The Substantive Origins of Criminal Procedure», *Yale Law Journal*, núm. 105, 1995, p. 393.

______«Warrants and Fourth Amendment Remedies», *Virginia Law Review*, núm. 77, 1991, p. 881.

SULLIVAN, Kathleen M. y GUNTHER, Gerald: *First Amendment Law*, Nueva York, Foundation Press, 1999.

SUNSTEIN, Cass: *Infortopia: How Many Minds Produce Knowledge*, Nueva York, Oxford University Press, 2006.

______*Legal Reasoning and Political Conflict*, Oxford, Oxford University Press, 1996.

______*Democracy and the Problem of Free Speech*, Nueva York, Free Press, 1995.

______*The Partial Constitution*, Cambridge (Mass.), Harvard University Press, 1993.

______«Legal Interference with Private Preferences», *University of Chicago Law Review*, núm. 53, 1986, p. 1129.

SWISHER, Kara: *Aol.com: How Steve Case Beat Bill Gates, Nailed the Netheads, and Made Millions in the War for the Web*, Nueva York, Times Business, 1998.

TEHRANIAN, John: «All Rights Reserved? Reassessing Copyright and Patent Enforcement in the Digital Age», *University of Cincinnati Law Review*, núm. 72, 2003, p. 45.

THOMSON, Judith J.: «The Trolley Problem», *Yale Law Journal*, núm. 94, 1985, p. 1395.

TIEBOUT, Charles M.: «A Pure Theory of Local Expenditures», *Journal of Political Economy*, núm. 64, 1956, p. 416.

TIEN, Lee: «Architectural Regulation and the Evolution of Social Norms», *International Journal of Communications Law and Policy*, núm. 9, 2004.

TOCQUEVILLE, Alexis de: *Democracy in America*, vol. 1, Nueva York, Vintage, 1990 [ed. cast.: *La democracia en América*, trad. por Raimundo Viejo Viñas, Madrid, Akal, 2007].

TORRES, Aida: «The Effects of Federal Funding Cuts on Family Planning Services, 1980–1983», *Family Planning Perspectives*, núm. 16, 1984, p. 134.

TRACHTMAN, Joel P.: «The International Economic Law Revolution», *University of Pennsylvania Journal of International Economic Law*, núm. 17, 1996, p. 33.

TRIBE, Laurence H.: «The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier», intervención en el Primer Congreso sobre Ordenadores, Libertad y Privacidad, 26 de marzo de 1991, reimpresa en *The Humanist*, septiembre-octubre de 1991, pp. 15–21.

______*American Constitutional Law*, Mineola (NY), Foundation Press, 1978.

TUCKER, St. George: *Blackstone's Commentaries 3*, South Hackensack (NJ), Rothman Reprints, 1969.

TURKLE, Sherry: *Life on the Screen: Identity in the Age of the Internet*, Nueva York, Simon & Schuster, 1995 [ed. cast.: *La vida en la pantalla: la construcción de la identidad en la era de Internet*, Barcelona, Paidós, 1997].

UNGAR, Sanford J.: *The Papers and the Papers: An Account of the Legal and Political Battle over the Pentagon Papers*, Nueva York, Columbia University Press, 1989.

US Department of Commerce, «Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights», 1995.

US Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, viii, 1973, citado en http://www.epic.org/privacy/consumer/code_fair_info.html.

VAIDHYANATHAN, Siva: «Remote Control: The Rise of Electronic Cultural Policy», *Annals of the American Academy of Political and Social Science*, vol. 597, núm. 1, 2005, p. 126.

VOLOKH, Eugene: «Freedom of Speech, Shielding Children, and Transcending Balancing», *Supreme Court Review*, 1997, p. 141.

VON HAYEK, Friedrich A.: *Law, Legislation, and Liberty*, vol. 2, Chicago, University of Chicago Press, 1978 [ed. cast.: *Derecho, legislación y libertad*, trad. por Luis Reig Albiol, Madrid, Unión Editorial, 1979].

WAGNER, R. Polk: «On Software Regulation», *Southern California Law Review*, núm. 78, 2005, pp. 457-516.

WALKER, Chip: «Can TV Save the Planet?», *American Demographics*, mayo de 1996, p. 42.

WALLACE, Jonathan y MANGAN, Mark: *Sex, Laws, and Cyberspace*, Nueva York, M&T Books, 1996.

WALZER, Michael: *Spheres of Justice: A Defense of Pluralism and Equality*, Nueva York, Basic Books, 1983 [ed. cast.: *Las esferas de la justicia: una defensa del pluralismo y la igualdad*, México, Fondo de Cultura Económica, 1997].

WEINBERG, Jonathan: «ICANN and the Problem of Legitimacy», *Duke Law Journal*, núm. 50, 2000, p. 187.

______«Cable TV, Indecency, and the Court», *Columbia-VLA Journal of Law and the Arts*, núm. 21, 1997, p. 95.

______«Rating the Net», *Hastings Communications and Entertainment Law Journal*, vol. 19, núm. 108, 1997, pp. 453-478.

WIENER, Norbert: *Cybernetics: Or Control and Communication in the Animal and the Machine*, Cambridge (Mass.), MIT Press, 1961 [1948] [ed. cast.: *Cibernética. O el control y comunicación en animales y máquinas*, trad. por Francisco Martín, Barcelona, Tusquets ed., 1985].

WILSON, Bradford P.: «The Fourth Amendment as More Than a Form of Words: The View from the Founding», en HICKOK Jr., Eugene W. (ed.): *The Bill of Rights: Original Meaning and Current Understanding*, Charlottesville, University Press of Virginia, 1991.

WINNER, Langdon: «Do Artifacts Have Politics?», en *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, Chicago, University of Chicago Press, 1986 [ed. cast.: *La ballena y el reactor: una búsqueda de los límites en la era de la alta tecnología*, trad. por Elizabeth Casals Bufano, Barcelona, Gedisa, 1987].

WOOD, Gordon S.: *The Radicalism of the American Revolution*, Nueva York, Alfred A. Knopf, 1992.

WU, Timothy: «When Code Isn't Law», *Virginia Law Review*, núm. 89, 2003, pp. 679–708.

ZDZIARSKI, Jonathan: *Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification*, San Francisco, No Starch Press, 2005.

ZELIZER, Viviana A.: *The Social Meaning of Money* (2ª), Princeton, Princeton University Press, 1994.

ZITTRAIN, Jonathan: *The Future of the Internet—And How to Stop It*, New Haven, Yale University Press, 2008.

______«The Generative Internet», *Harvard Law Review*, núm. 119, 2006, p. 1974.

______«What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication», *Stanford Law Review*, núm. 52, 2000, p. 1201.

______«The Rise and Fall of Sysopdom», *Harvard Journal of Law and Technology*, núm. 10, 1997, p. 495.

ZUCKER, Lynne G.: «Production of Trust: Institutional Sources of Economic Structure, 1840-1920», *Research in Organizational Behavior*, núm. 8, 1986, p. 53.

20. Producción cultural y prácticas instituyentes
Líneas de ruptura en la crítica institucional
transform
245 pp., 15 euros.

21. Postmetrópolis
Estudios críticos sobre las ciudades y las regiones
Edward S. Soja
594 pp., 35 euros.

22. Mil máquinas
Breve filosofía de las máquinas como movimiento social
Gerald Raunig
126 pp., 10 euros.

23. Deseo (y) libertad
Una investigación sobre los presupuestos de la acción colectiva
Montserrat Galcerán
208 pp., 14 euros.

historia

1. Lo queremos todo
Nanni Balestrini
ISBN: 84-96453-08-1. 172 pp., 12 euros

2. 68
Paco Ignacio Taibo II
ISBN: 84-96453-09-X. 110 pp., 10 euros

3. Autogestión y anarcosindicalismo
en la España revolucionaria
Frank Mintz
I.S.B.N.: 84-96453-07-3. 300 pp., 18 euros.

4. Techno Rebelde
Un siglo de músicas electrónicas
Ariel Kyrou
I.S.B.N.: 84-96453-10-3. 400 pp., 20 euros.

5. La horda de oro
La gran ola creativa y existencial, política y revolucionaria (1968-1977)
Primo Moroni y Nanni Balestrini
I.S.B.N.: 84-96453-13-8. 680 pp., 28 euros.

6. Los invisibles
Nanni Balestrini
I.S.B.N.: 84-96453-29-4. 304 pp., 15 euros.

7. Las huelgas en Francia durante mayo y junio de 1968
Bruno Astarian
I.S.B.N.: 978-84-96453-23-4. 176 pp., 12 euros.

8. Luchas autónomas en los años setenta
Del antagonismo obrero al malestar social
Espai en Blanc (coord.)
I.S.B.N.: 978-84-96453-30-2. 368 pp., 18 euros.

bifurcaciones

1. Lo que el trabajo esconde
Materiales para un replanteamiento del análisis sobre el trabajo
B. Lahire, P. Rolle, P. Saunier, M. Stroobants, M. Alaluf, M. Postone
ISBN: 84-933555-6-9. 264 pp., 18 euros

2. Marx Reloaded
repensar la teoría crítica del capitalismo
Moishe Postone
ISBN: 978-84-96453-21-9. 208 pp., 16,50 euros

3. De la revolución del trabajo al trabajo revolucionado
Investigaciones sobre las transformaciones de la Unión Soviética y Rusia
Pierre Rolle
ISBN: 978-84-96453-35-7. 240 pp., 17 euros